FORM PTO-1390 (Modified) (REV 5-93) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 051508/0103

U.S. APPLICATION NO. (If known, see 37 C F.R 1.5): 09/194,051

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/JP97/00972	**March 24, 1997**	**March 24, 1997**

TITLE OF INVENTION
UNIQUE TIME GENERATING DEVICE AND AUTHENTICATING DEVICE USING THE SAME

APPLICANT(S) FOR DO/EO/US
Akira SUGIYAMA

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371 (c)(2)).

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☐ Other items or information:

U.S APPLICATION NO. (If known, see 37 C F R 1 50	INTERNATIONAL APPLICATION NO. PCT/JP97/00972	ATTORNEY'S DOCKET NUMBER 051508/0103

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5):		
Search Report has been prepared by the EPO or JPO **$840.00**		
International preliminary examination fee paid to USPTO (37 CFR 1.482) **$670.00**		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2) **$760.00**		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$970.00**		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) **$96.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ **840.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e))	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	**39** -20 =	**19**	X **$18.00**	$ **752.00**	
Independent Claims	**6** -3 =	**3**	X **$78.00**	$ **234.00**	
Multiple dependent claim(s) (if applicable)			+ **$260.00**	$ **0.00**	
TOTAL OF ABOVE CALCULATIONS =				$ **1,826.00**	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$ **0.00**	
SUBTOTAL =				$ **1,826.00**	
Processing fee of **$130.00** for furnishing English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f). +				$ **0.00**	
TOTAL NATIONAL FEE =				$ **1,826.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ **0.00**	
TOTAL FEES ENCLOSED =				$ **1,826.00**	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of **$1,826.00** to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. 19-0741 in the amount of $ to the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 19-0741. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Foley & Lardner
3000 K Street, N.W., Suite 500
P.O. Box 25696
Washington, D.C. 20007-8696

Reg No. 35,050
SIGNATURE

Arthur Schwartz
NAME

22,115
REGISTRATION NUMBER

Form PTO-1390 (REV 5-93) (Modified)

Applicant or Patentee: Akira SUGIYAMA
Serial or Patent No.: _____ Atty. Dkt. No. 051508/0103
Filed or Issued: November 23, 1998
For: UNIQUE TIME GENERATING DEVICE AND AUTHENTICATING DEVICE USING THE SAME

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) AND 1.27 (c)) — INDEPENDENT INVENTOR

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled UNIQUE TIME GENERATING DEVICE AND AUTHENTICATING DEVICE USING THE SAME, described in

( ) the specification filed herewith
(XX) application serial no. PCT/IP97/00972, filed March 24, 1997
( ) patent no. _____, issued _____

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey, or license any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below.

( ) no such person, concern or organization
( ) persons, concerns or organizations listed below*

*** NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)**

FULL NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT CORPORATION

FULL NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT CORPORATION

FULL NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT CORPORATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate: (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Akira SUGIYAMA		
NAME OF INVENTOR	NAME OF INVENTOR	NAME OF INVENTOR
Signature of Inventor	Signature of Inventor	Signature of Inventor
A. Sugiyama		
Date December 9, 1998	Date	Date

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 051508/0103

In re patent application of
Akira SUGIYAMA
Serial No. Unassigned
Filed: November 17, 1998
For: UNIQUE TIME GENERATING DEVICE AND AUTHENTICATING DEVICE USING THE SAME

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination of the above-identified application, Applicant respectfully requests that the following amendments be entered into the application:

IN THE CLAIMS:

Please amend the claims as follows:

Claim 6, delete "or 4".

Claim 7, delete "or 4".

Claim 8, line 2, delete "any one of the preceding claims", and insert --claim 1--.

Claim 9, line 2, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 10, line 2, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 11, lines 3 and 4, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 14, line 2, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 15, line 2, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 16, line 2, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 17, line 2, delete "any one of claims 1 to 7", and insert --claim 1--.

Claim 32, delete "or 31".

Please rewrite the following claims:

36. (Amended) An authentication-data issuing system as recited in [any one of claims 14 to 17] claim 14 wherein the unique authentication data created and issued by said subservient computer contains the unique authentication data updated by [said] renewal means [recited in claim 34].

38. (Amended) An authentication-data issuing system as recited in claim 37 wherein the recording media having stored thereon updated unique authentication data is [the] a ticket [recited in claim 18], a prepaid card [recited in claim 19], an electronic money [recited in claim 20], an ID card [recited in claim 21], or a card [recited in claim 22], and wherein the subservient

computer that stores the updated unique authentication data on said recording media is contained in or attached to an automatic ticket checker or a card reader/writer for [a] the prepaid card, the ID card or the electronic money.

REMARKS

Entry of the foregoing amendments prior to examination is respectfully requested.

Applicant respectfully requests that the foregoing amendments to Claims 6-11, 14-17, 32, 36, and 38 be entered in order to avoid this application incurring a surcharge for the presence of one or more multiple dependent claims.

Respectfully submitted,

November 23, 1998

Arthur Schwartz
Reg. No. 22,115

FOLEY & LARDNER
3000 K Street, N.W.
Suite 500
Washington, D.C. 20007-5109
Tel: (202) 672-5300

DESCRIPTION

AUTHENTICATION-DATA ISSUING SYSTEM BASED ON UNIQUE TIME, RECORDING MEDIA FOR STORING AUTHENTICATION DATA ISSUED BY THE AUTHENTICATION-DATA ISSUING SYSTEM AND AUTHENTICATION DATA VERIFYING SYSTEM

TECHNICAL FIELD

The present invention relates to an authentication data issuing system based on unique time generation, a recording media for storing authentication data issued by the authentication-data issuing system and an authentication data verifying system, which exercise general control of information issued by particular computers, verify authentication data issued by some of the computers and thereby effectively avoid damages that would be caused by any person stealing the authentication data.

BACKGROUND ART

Today, various prepaid cards, each prestoring money amount information corresponding to a certain amount of money paid in advance, are being widely used in various commercial transactions, such as for using railroad facilities and public telephones and playing with Japanese pinball (hereinafter "pachinko") game machines. These prepaid cards are inserted into card reader/writers

attached to or contained in various pieces of equipment, such as automatic ticket checkers, automatic ticket vending machines, public telephones and game machines, where each amount due is subtracted from the remaining balance on the card and the prestored money amount information is rewritten accordingly.

Besides, in various banking agencies and the like, account transfer services using personal computers and public telephone lines have come into wide use, and it is expected that every banking and currency settlement service will be conducted through an electronic currency system in the near future (as disclosed in, for example, Japanese Patent Publication No. HEI-7-11723).

Recently, an increasing number of persons have been attempting to tamper or copy the stored data on the prepaid cards without due authorization, so that prepaid card issuing companies are exercising, against such fraudulent attempts, preventive measures that include encryption and scrambling of the stored data. In the account transfer and various electronic business transactions, many persons have been attempting to acquire other person's authentication data in a fraudulent manner, in order to make unfair benefits by pretending to be the true prepaid card holder.

DISCLOSURE OF THE INVENTION

The present invention has been made in view of

such inconveniences encountered by prior techniques and seeks to provide an improved technique which, using a unique time generating device previously proposed by the applicant of the present application (in PCT/JP/02433), can effectively avoid damages that would be caused by any person stealing authentication data.

In order to accomplish the above-mentioned object, the present invention provides an authentication-data issuing system based on unique time, the authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of the computers set to function as a master computer, the master computer comprising: a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating the unit time values output by the time keeping means so as to constantly measure a changing elapsed time within the time-measuring period; transmitter means for, during communication between the master computer and another of the computers subservient to the master computer, transmitting, from the master computer to the subservient computer, authentication data based on an elapsed time measurement, corresponding to a

given time point, indicated by the unique time generating device; and register means for receiving and registering an issuance history of unique authentication data created and issued by the subservient computer imparting additional data, unique to the subservient computer, to the authentication data transmitted by the master computer.

According to another aspect of the present invention, there is provided an authentication-data issuing system based on unique time, the authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of the computers set to function as a master computer, the master computer including a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating the unit time values output by the time keeping means so as to constantly measure a changing elapsed time within the time-measuring period. Each of the computers subservient to the master computer comprises: receiver means for, during communication with the master computer, receiving authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by the unique time generating

device of the master computer; issuer means for creating and issuing unique authentication data by imparting additional data, unique to the subservient computer, to the authentication data received via the receiver means from the master computer; and transmitter means for transmitting, to the master computer, an issuance history of the unique authentication data created and issued by the issuer means.

According to still another aspect of the present invention, there is provided an authentication-data issuing system based on unique time, the authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of the computers set to function as a master computer, where each of the computers subservient to the master computer comprises: a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period unique to the computer that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating the unit time values output by the time keeping means so as to constantly measure a changing elapsed time within the time-measuring period; issuer means for creating and issuing unique authentication data, peculiar to the subservient computer, on the basis of an elapsed time

measurement indicated by the unique time generating device; and transmitter means for transmitting, to the master computer, an issuance history of the unique authentication data created and issued by the issuer means.

According to still another aspect of the present invention, there is provided an authentication-data issuing system based on unique time, the authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of the computers set to function as a master computer. Each of the computers subservient to the master computer comprises a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period unique to the computer that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating the unit time values output by the time keeping means so as to constantly measure a changing elapsed time within the time-measuring period. The master computer, exercising general control of the subservient computers, includes register means for receiving and registering an issuance history of data created and issued by each of the subservient computers on the basis of an elapsed time measurement indicated by the unique time generating device of the subservient

computer.

According to still another aspect of the present invention, there is provided a recording media having stored thereon unique authentication data created by any one of the subservient computers, and the recording media is issued by the subservient computer.

According to still another aspect of the present invention, there is provided an authentication-data verifying system including a plurality of computers connected with each other via communication lines with one of the computers set to function as a master computer. Each of the computers subservient to the master computer comprises: reading means for reading unique authentication data issued by any one of the subservient computers on the basis of information received from another of the subservient computers, or reading unique authentication data issued by any one of the subservient computers and recorded on a recording media; transmitter means for transmitting the unique authentication data read by the reading means to the master computer for subsequent collation thereby; and receiver means for receiving from the master computer a result of collation between an issuance history of the unique authentication data by each of the subservient computers registered in the master computer and the unique authentication data transmitted by the transmitter means.

According to still another aspect of the present invention, there is provided an authentication-data verifying system including a plurality of computers connected with each other via communication lines with one of the computers set to function as a master computer, where the master computer comprises: receiver means for receiving unique authentication data transmitted by transmitter means of any one of the computers subservient to the master computer, the unique authentication data being issued by the subservient computer and read by reading means of the subservient computer; and collator means for collating between the unique authentication data received by the receiver means and an issuance history of the unique authentication data by each of the subservient computers that is registered in the master computer; and transmitter means for transmitting a result of collation by the collator means to receiver means of the subservient computer.

DESCRIPTION OF THE DRAWINGS

Fig. 1 is a network diagram illustrating an authentication-data issuing system, according to a best mode of carrying out the present invention, for issuing prepaid cards to be used for pachinko game machines;

Fig. 2 is a block diagram illustrating a general setup of a unique time generating device employed in the authentication-data issuing system of Fig. 1;

Fig. 3 is a diagram explanatory of a manner in which an elapsed time is measured in accordance with the best mode of the present invention;

Fig. 4 is a diagram showing examples of different time-measuring periods assigned to a plurality of unique time generating devices provided in a plurality of computers;

Fig. 5 is a diagram showing other examples of different time-measuring periods assigned to other unique time generating devices;

Fig. 6 is a block diagram illustrating a general organization of a master computer shown in Fig. 1;

Fig. 7 is a diagram illustrating contents of authentication data transmitted from the master computer of Fig. 1;

Fig. 8 is a block diagram illustrating a general organization of a card distributor's computer of Fig. 1;

Fig. 9 is a diagram illustrating contents of authentication data issued from a card distributor's computer to a pachinko house of Fig. 1;

Fig. 10 is a diagram illustrating a processing flow for creating unique authentication data;

Fig. 11 is a block diagram illustrating a general organization of a pachinko game machine shown in Fig. 1;

Fig. 12 is a diagram illustrating a processing flow for creating unique-authentication-data updating;

Fig. 13 is a diagram illustrating contents of

information presented on a display means when a card is used with updated data;

Fig. 14 is a diagram illustrating a hierarchical network of an authentication-data issuing system according to Example 1 installed within a company;

Fig. 15 is a block diagram illustrating a general organization of a master computer shown in Fig. 14;

Fig. 16 is a block diagram illustrating a general organization of a lower-level computer subservient to the master computer shown in Fig. 14;

Fig. 17 is a diagram illustrating a hierarchical network of an authentication-data issuing system according to Example 2;

Fig. 18 is a diagram illustrating a hierarchical network of an authentication-data issuing system according to Example 3;

Fig. 19 is a diagram illustrating a hierarchical network of an authentication-data issuing system according to Example 4; and

Fig. 20 is a diagram illustrating a hierarchical network of an authentication-data issuing system according to Example 5.

BEST MODE FOR CARRYING OUT THE INVENTION

In PCT Patent Application No. PCT/JP/02433 filed at an earlier date, the applicant of the present application proposed a unique time generating device and

fully explained the concept of "unique time" generated by the device. Unlike the today's commonly-used time concept based on Greenwich Mean Time, the "unique time" is a time concept to linearly count a preset finite time period from the zeroth toward the last second thereof, i.e., to constantly a measure changing elapsed time toward the last second within the preset time-measuring period.

On the basis of such a unique time concept, the present invention provides for authentication of a given computer on a communication network or authentication of a recording media storing thereon authentication data issued by a given computer on the communication network. First, the present invention will be described hereinbelow in relation to a system for issuing and authenticating prepaid cards for use in Japanese pinball, i.e., "pachinko", game machines equipped with card readers (commonly known as CR-type pachinko game machines).

In Fig. 1, reference numeral 1 represents a highest-level master computer of an original card issuer company that issues prepaid cards (prepaid pachinko cards), to which are connected, via network lines, subservient second-level computers 2A, 2B, 2C, ..., 2n of card distributor companies. Further, to the second-level computers 2A, 2B, 2C, ..., 2n of the card distributor companies are connected host computers (such as those

denoted at 3A, 3B, ..., 3n) of affiliated pachinko houses. In each of the pachinko houses, the host computer (such as 3A) collectively manages or exercising general control of individual pachinko (CR-type) pachinko game machines 4 and prepaid card vending machines 5 located within the house. In addition, in each of the pachinko houses, third-level computers are provided within or connected with the host computer (such as 3A).

The above-mentioned highest-level master computer 1 implements a unique time generating device 6 as shown in Fig. 2 by arranging its CPU 7 to provide a time keeping means 9 and accumulating means 10 and also setting a memory 8 to include a storage means 11 for storing a preset time-measuring period and a renewal means 12 for renewing the time-measuring period. Total time value to be counted over the preset time-measuring period may be optionally set, for example, to correspond to a total value of seconds over a period of ten or 100 years, and every elapsed time within the preset time-measuring period is measured by the time keeping means 9 constantly counting the total time value. For example, the total time values for one, ten and 100 years will be as follows:

Total time value to be counted over a one year period = 31,556,925.9747 seconds (one year = 365.2425 days);

Total time value to be counted over a ten

year period = 315,659,250.9747 seconds; and

Total time value to be counted over a 100 year period = 3,155,692,500.9747 seconds

Here, the "total time value to be counted" is expressed in time units of 1/10,000 second measured by an atomic clock (cesium clock), and a "unique time" is given by constantly counting the total time value to identify a changing elapsed time within the preset time-measuring period. Elapsed time (unique time measurement) is typically calculated from both an accumulated time and a subtracted time, as shown in Fig. 3. Specifically, the accumulated time is a time value measured forward or incrementally from the zeroth second toward the total time value to be counted, while the subtracted time is a time value measured rearward or decrementally from the total time value toward the zeroth second. Alternatively, a unique time measurement may be calculated from either the accumulated time or the subtracted time or by adding some variables to the time value.

The accumulating means 10 sequentially accumulates successive unit time values measured the time keeping means 9; that is, the accumulating means 10 calculates an accumulated time Tn from the zeroth second toward the last second of the total time value Tt to be counted as well as a subtracted time from the last second toward the zeroth second (Tt - Tn), so as to constantly provide

a changing elapsed time within the preset time-measuring period (see Fig. 3). Once the time value accumulated by the accumulating means 10 has reached the predetermined total time value to be counted Tt (i.e., once the counting of all the seconds in the 100 year period has been completed), the time period renewal means 12 in the memory 8 is activated to renew the time-measuring period for another 100 years and instructs the time keeping means 9 to count the renewed time-measuring period. In this way, the unique time generating device provided in the computer is updated once for every 100 years.

Similar unique time generating device is provided in each of the second-level computers 2A, 2B, ..., 2n of card distributor companies A to n directly connected to or subservient to the highest-level master computer 1, the third-level computers 3A, 3B, ..., 3n of the pachinko houses connected to the second-level computers 2A, 2B, ..., 2n and the fourth-level computers of the individual pachinko game machines 4 and prepaid card vending machines 5 connected to the third-level computers 3A, 3B, ..., 3n. All these unique time generating devices provided in the above-mentioned computers are set to indicate unique elapsed time measurements, different from each other, at every given point. For example, as seen from "product 1" to "product n" in Fig. 4, the unique time generating devices are sequentially produced, at intervals of, for example, one second, and they are

set to start measuring time at different points that depend on the production intervals and thus differ in measured elapsed time from each other by one second; for the same reason, they are set to end measuring time at different points that are displaced from each other by one second due to the differences of their time-measurement start points, although the total time value to be counted Tt, i.e., the length of the time-measuring period (e.g., 3,155,692,500.97 seconds), is the same for all the products, i.e., unique time generating devices. Alternatively, the length of the time-measuring period may be made different among these products or unique time generating devices. As shown in Fig. 5, the unique time generating device 6 provided in the master computer 1 may be set as a master device and the total time values Tt of product 1 to product n sequentially produced or supplied on the basis of unique time generation by the master device may be set to progressively become great relative to that of the master device in such a way that each of the products has a total time value Tt greater by one second than that of the preceding product. It may be assumed that all these unique time generating devices including the master device are caused to start measuring time like a stopwatch. This way, all the unique time generating devices including the master device are allowed to start measuring at a same start point up to their unique total

time values (i.e., up to the end of different time-measuring periods); thus, they stop the counting at different end points that will sequentially arrive every second. As a result, all the unique time generating devices indicate different elapsed time measurement at every given time point within the different time-measuring periods, as shown in Fig. 5.

As clearly shown in Fig. 6, the highest-level master computer 1 includes a transmitter means 13 that transmits, to the respective computers 2A, 2B, ..., 2n of the card distributor companies, authentication data based on an elapsed time measurement at a given time point indicated by the unique time generating device 6 thereof. Let's assume here that the master computer 1 generates original authentication data X1a, X2a and X3a (Fig. 7) corresponding to elapsed times measured by the unique time generating device 6 and sequentially issues these original authentication data X1a, X2a and X3a to one of the second-level computers (e.g., computer 2A). Specifically, each of the thus-issued original authentication data X1a, X2a and X3a is transmitted to the second-level computer (e.g., computer 2A), where it is used as identification (ID) data to authorize issuance of a prepaid card, i.e., issuance-authorizing identification data (see Fig. 7).

More specifically, each of the original authentication data X1a, X2a and X3a transmitted by the

transmitter means 13 of the master computer 1 is received by the second-level computer of one of the card distributors requesting the issuance (e.g., card distributor A). As shown in Fig. 8, this second-level computer 2A of card distributor A also includes a CPU 15, a memory 16 having provided therein the unique time generating device 2A6, a receiver means 17 and a transmitter means 18. Each of the original authentication data X1a, X2a and X3a received by the receiver means 17 of the second-level computer is temporarily stored into a register means 19 within the memory 16 and then read out from the register means 19 upon request from the host computer of any one of the pachinko houses. If the receiver means 17 of the second-level computer 2A receives a request for issuance of authentication data for 1,000 1,000-YEN-worth prepaid cards, 100 5,000-YEN-worth prepaid cards and 20 10,000-YEN-worth prepaid cards, then the computer 2A reads out the authentication data X1a, X2a and X3a from the register means 19 and imparts thereto unique additional authentication data A1 - A1000, B1 - B100 and C1 - C20, respectively, that are based on elapsed time measurements sequentially output by the unique time generating device 2A6 of the computer 2A. In this way, unique authentication data corresponding to the respective numbers of the 1,000-YEN, 5,000-YEN and 10,000-YEN prepaid cards are created on the basis of elapsed time

measurements sequentially output by the unique time generating device 2A6; that is, the authentication data of the 1,000-YEN prepaid cards will be X1a+A1 to X1a+A1000, the authentication data of the 5,000-YEN prepaid cards will be X2a+B1 to X2a+B100, and the authentication data of the 10,000-YEN prepaid cards will be X3a+C1 to X3a+C20. The thus-created authentication data are then transmitted from the transmitter means 18 of the second-level computer 2A to the host computer 3A of the pachinko house A. At the same time, the computer 2A of card distributor A erases the identification, actually issued to the pachinko house's host computer (e.g., host computer 3A), from among the issuance-authorizing identifications corresponding to the authentication data X1a, X2a and X3a. Once the identification authorizing issuance of a prepaid card (issuance-authorizing identification) has run out as a result of the erasure, new original authentication data are supplied by the master computer 1.

In each of the pachinko houses (the following description will be made primarily about the pachinko house A), the receiver means of the host computer 3A receives the authentication data (e.g., X1a+A1, X2a+B1 and X3a+C1) transmitted by the card distributor A. The host computer of each of the pachinko houses is constructed in a similar manner to the second-level computer of Fig. 8 and imparts, to the received

authentication data (e.g., X1a+A1, X2a+B1 and X3a+C1), identification based on elapsed time measurements sequentially indicated by the unique time generating device 3A6 of the host computer. Further, in each of the vending machines 5 capable of dispensing 1,000-YEN, 5,000-YEN and 10,000-YEN prepaid cards to customers, the unique time generating device (e.g., 5A1-6) provided in its computer imparts additional identification data based on elapsed time measurements sequentially indicated thereby. Thus, the vending machine 5 in pachinko house A can sell, to customers, prepaid magnetic cards 20 which have stored thereon unique authentication data (X1a+A1+3A****+5A****) as a result of sequential impartment of various unique data based on the respective elapsed time measurements indicated by the unique time generating devices at various hierarchical levels, as shown in Fig. 10.

The ultimate unique authentication data thus recorded on each of the prepaid cards 20 (X1a+A1+3A****+5A****) is transmitted from the lowest-level computer of the vending machine 5 to the receiver means of the host computer 3A of the pachinko house A, which in turn identifies, from the recorded ultimate unique authentication data, an up-to-date record or history of prepaid card issuance by the vending machine 5 and transmits the ultimate unique authentication data to the receiver means 17 of the second-level computer 2A of

card distributor A shown in Fig. 8. The second-level computer 2A of card distributor A receives, by means of its receiver means 17, the ultimate unique authentication data transmitted from all the associated pachinko houses and stores them into the register means 19 thereof, via which the computer 2A transmits the ultimate authentication data to the receiver means 14 of the highest-level main computer 1. Then, the master computer 1 receives the ultimate unique authentication data transmitted from the computers 2A to 2n of the individual card distributor companies and stores them in the register means 21 within the memory 8.

Note that each of the master computer 1 and subservient computers 2A and 3A of card distributor A and pachinko house stores the received ultimate unique authentication data after collating it with the corresponding authentication data (issuance-authorizing identification) previously sent to the subservient computers. Also, the master computer 1 has prestored therein various attributes of the unique time generating devices provided therein and in all the subservient computers as shown in Fig. 5, so that the master computer 1 rejects the registration, in its register means, of any ultimate unique authentication data containing an attribute that does not agree with the prestored attributes.

In the above-mentioned manner, each of the prepaid

cards 20 sold by vending machine 1 of pachinko house A can be used as a common card universally usable in all the pachinko houses under the control of card distributor company A or of the master computer 1; for example, the issued prepaid card 20 can be used for "pachinko game machine 4" in pachinko house A.

The pachinko game machine of each of pachinko houses A to n ((the following description will be made primarily about pachinko game machine 4) includes a card reader/writer 22 contained in or connected to the lowest-level computer of pachinko game machine 4 as shown in Fig. 11. Reading means 23 of the computer in Fig. 11 reads the ultimate unique authentication data recorded on the prepaid card 22 that is inserted in the card reader/writer 2. The ultimate unique authentication data (X1a+A1+3A****+5A****) read out from the prepaid card 22 by the reading means 23 is transmitted from the transmitter means 24 of the computer to the host computer 3A of pachinko house A. The ultimate unique authentication data received by the receiver means of the host computer 3A is then forwarded, through the receiver means 17 of the computer 2A of card distributor A, to the receiver means 14 of the master computer 1 for necessary collation. The computer 2A of card distributor A or the master computer 1 includes a collator means 26 or 27 as shown in Fig. 6 or 8, which determines whether the ultimate unique authentication data (X1a+A1+3A****+5A*

) received by the receiver means 14 or 17 has been duly registered in the up-to-date record or history of issuance in the register means 19 or 21. When, for example, the collator means 27 in the computer 2A of card distributor A determines that the unique authentication data received from the subservient computer (host computer 3A of pachinko house A) does not match the data stored in the register means 19, the unique authentication data is transmitted from the transmitter means 18 of the computer 2A to the receiver means 14 of the master computer 1, where the data is collated by the collator means 26. Thus, as long as the collator means 26 or 27 of the master computer 1 or the computer 2A of card distributor A determines that the unique authentication data (X1a+A1+3A*+5A****) received from the subservient computer (host computer 3A of pachinko house A) matches the data stored in the register means 19 or 21, the means 26 or 27 passes the determination or collation result, through the host computer 3A, to the computer of the pachinko game machine. Finally, the collation result is received by the receiver means 25 shown in Fig. 11. The collation result, of the inserted prepaid card, by the collator means 26 or 27 thus received by the receiver means 25 is visually shown on a display 28 of pachinko game machine 4 shown in Fig. 11. If, for example, the prepaid card 20 inserted in the card reader/writer 22 is collated

with the registered data and determined, by the collator means 26 or 27 of the higher-level computer, as being a genuine or authentic card rightly issued by any one of the computers under the control of the master computer 1, an authorizing means 29 accepts the prepaid card 20 as authentic and displays various information, such as the type, issue date and remaining units, of the card (see Fig. 11) on the display that is typically in the form of an LCD (Liquid Crystal Display) or CRT (Cathode Ray Tube). If, on the other hand, the prepaid card 20 inserted in the card reader/writer 22 is collated with the registered data, determined, by the collator means 26 or 27 of the higher-level computer, as not matching the data stored in the register means 19 or 21 and such a collation result is received by the receiver means 25, a rejecting means 30 determines the inserted prepaid card 20 as not being an authentic card rightly issued by any one of the computers under the control of the master computer 1 and displays a rejection message "This card is unusable." on a display 28A in the form of an LCD or CRT; in this case, the rejecting means 30 also instructs the card reader/writer 22 to reject the card as false.

The prepaid card 20 determined as authentic or acceptable by the authorizing means 29 can be used in pachinko game machine 4 by the holder or user of the card. Specifically, if the user, holding a 1,000-YEN prepaid card 20, selectively depresses one of a plurality

of buttons on pachinko game machine 4 to purchase pachinko balls for 500 YEN (50 units) while referring to the information of the card 20 shown on the display 28, the selected purchase information is transmitted from the pachinko game machine's computer, through the host computer 3A of pachinko house A and computer 2A of card distributor A, to the master computer 1 in association with the ultimate unique authentication data stored on the card 20.

In the master computer 1 having received the selected purchase information, a renewal means 31 first confirms that the unique authentication data (X1a+A1+3A******+5A****) received in association with the selected purchase information matches the data previously stored in the register 21 and then creates identification (ID) to authorize the selected purchase. As shown in Fig. 12, the purchase-authorizing ID is created, as authentication-data-updating data Y1a, on the basis of an elapsed time measurement Y1 indicated by the unique time generating device 6 provided in the master computer 1, and the thus-created authentication-data-updating data Y1a is then transmitted from the receiver means 13 to the second-level computer 2A along with the unique authentication data (X1a+A1+3A****+5A****).

Similarly, in the second-level computer 2A of card distributor A, a renewal means 32 first confirms that the unique authentication data matches the data stored in

the register 19 and then creates identification data to authorize the selected purchase. As shown in Fig. 12, the purchase-authorizing ID is created, as authentication-data-updating data P1a, on the basis of an elapsed time measurement P1 indicated by the unique time generating device 2A6 provided in the computer 2A, and the thus-created authentication-data-updating data P1a is then transmitted from the receiver means 18 to the host computer 3A subservient to the computer 2A along with the authentication data Y1a created by the master computer 1.

In the host computer 3A as well, further authentication-data-updating data Q1a is created on the basis of a current elapsed time measurement Q indicated by the unique time generating device 3A6 and added to the received data (Y1a+P1), and the added result is transmitted to the pachinko game machine 4. Finally, in the pachinko game machine 4, further authentication-data-updating data R1a is created on the basis of a current elapsed time measurement R1 indicated by the unique time generating device 4A1-6 provided in its computer and added with the data Y1a, P1a and Q1a to provide ultimate authentication-data-updating data (Y1a+P1a+Q1a+R1a), as shown in Fig. 12.

In the computer of the pachinko game machine 4, a renewal means 33 updates the last-stored unique authentication data (X1a+A1+3A****+5A****) on the prepaid

card 20, on the basis of the updating data (Y1a+P1a+Q1a+R1a); the updating may be done by erasing the last unique authentication data or adding thereto the updating data. What is essential here is that the last-stored unique authentication data should be altered on the basis of the updating data (Y1a+P1a+Q1a+R1a). The alteration of the unique authentication data is effected via the card reader/writer 22, and thus the prepaid card 22 is discharged from the reader/writer 22 with its unique authentication data altered on the basis of the updating data corresponding to the selected purchase of pachinko balls for 500 YEN (50 units).

The altered data (updated unique authentication data) is transmitted to the higher-order computers, one after another, in the hierarchical network structure. Thus, in the computer 2A of card distributor A, the renewal means 32 replaces the last unique authentication data, registered in the register means 19, with the updated unique authentication data. Then, in the master computer 1 as well, the renewal means 31 replaces the last unique authentication data, registered in the register means 21, with the updated unique authentication data. In this way, the up-to-date record or history of issuance of the unique authentication data by each of the higher-order computers is updated.

Next time the prepaid card 20 is used at any one of the pachinko game machines under the control of the

master computer 1, the updated unique authentication data is read out from the card 20 and collated with the data stored in the registers 19 and 20 of the upper-order computers to ascertain its acceptability, in a similar manner to the above-mentioned. At this time, data indicative of the most recent use of the card 20 is displayed on the display 28 of the pachinko game machine 28, as shown in Fig. 13.

As described above, according to the prepaid card issuing and authenticating system, each of the pachinko houses under the control of the master computer 1 imparts, to every inserted prepaid card 20, additional authentication data that is based on respective elapsed time measurements indicated by the individual unique time generating devices, so that various data relating to the issuance and use of the card can be recorded on the card substantially in a time-series fashion. Therefore, every issued prepaid card will have an utterly unique identification and its recorded data will be updated upon insertion into the reader/writer 22. Thus, in a situation where 1,000 or 10,000 false prepaid cards are fabricated which have same data as recorded on a fairly issued authentic card and when someone actually inserts one of the cards into a pachinko game machine, the recorded data on the inserted card is updated in the above-described manner, so that all of the other cards than the initially inserted one will be automatically

rejected as unusable or unacceptable (the original authentic card will also be rendered unusable). With such an arrangement, unfair alteration or tampering or forgery of prepaid cards will end in meaningless effort and thus a thorough self-defense (i.e., safeguard against unfair transfer of the cards to other persons and theft of the cards) is achieved by the present invention.

Whereas the authentication-data-updating data are passed downward to the fourth-level computer in the above-described best mode as shown in Fig. 12, such updating data may be passed from the fourth-level computer upward to the higher-order computers so that same authentication-data-updating data is ultimately shared between the master computer 1 and the fourth-level computer and a prepaid card is issued with the updated unique authentication data. Further, whereas the above-described best mode is arranged such that the data to rewrite data to be recorded on a prepaid card 20 is transmitted to the higher-order computers after the necessary collation is performed on the card 20 inserted in the card reader/writer 22 and then the card 20 is judged to be a fairly issued card, it is preferable that such information exchanges be conducted collectively at one time.

Moreover, whereas in the above-described best mode the unique time generating device is provided in each of the computers of the card distributors, pachinko houses

and vending machines and pachinko game machines of the pachinko houses, all of these computers need not necessarily contain such a unique time generating device. Namely, in one alternative, the subservient computers under the control of the master computer 1 may impart, to authentication data based on an elapsed time measurement and received from the master computer 1, respective unique additional data (differing among the computers) so that unique authentication data created by combining these unique data is recorded on a prepaid card 20 to be newly issued or updated (as recited in claims 2 and 8 appended hereto). In this case, it is preferable that the master computer 1 at the highest level in the hierarchical structure should prestore the respective unique additional data of the individual subservient computers so as to be able to ascertain via which of the channels has been issued the unique authentication data ultimately recorded on the card 20 and registered or updated in the register means 21 (as recited in claim 8 appended hereto).

Furthermore, the subservient computers under the control of the master computer 1 have been described above as providing the unique time generating devices that indicate different elapsed time measurements at every given time point. Each of these unique time generating devices may be implemented by a software program installed in the corresponding computer, or may

be provided on an IC chip built in the computer, or may be a discrete driver or generator external to the computer. Further, the unique time generating device may be provided in each of the subservient computers under the control of the master computer 1 with the master computer 1 or owner of the computer 1 operating as an initial or original card supplier (as recited in appended claims 6 and 7). Namely, if the initial card supplier is arranged to prestore contents of data to be generated by the individual unique time generating devices which include their respective elapsed time measurements as well as their respective attributes relative to the master computer 1, it is possible to ascertain via which procedure has been issued the unique authentication data ultimately recorded on the card 20 and registered or updated in the register means 21 (as recited in appended claim 8). In addition, the computer of each of the card distributors may be set to operate as a secondary supplier which supplies the lower-order computers with unique time measurements received from the master computer 1.

In the above-described best mode, each of the vending machines 5 and pachinko game machines 4 has a computer or unique time generating device. Alternatively, without employing such a system, the host computer of each of the pachinko houses may be set to operate as a lowest-level computer which collectively

controls the individual vending machines 5 and pachinko game machines 4. In this case, the host computer creates and update the unique authentication data and then records the authentication data on a prepaid card that is issued by the vending machine 5 and used in the pachinko game machine 4.

The highest-level computer in the hierarchical structure has been described above as the "master computer" 1 controlling a plurality of other computers. In this sense, any one of the computers of the card distributors and host computers of the pachinko houses may be set to function as the master computer.

Furthermore, the best mode has been described above in relation to prepaid cards for use in pachinko game machines, the present invention may be applied to other prepaid card instruments, such as those for railroads, ships, airplanes, telephones, amusement parks (as recited in appended claim 9). In this case, the system according to the above-described best mode may be provided in the host computers of the card distributors or in the computers of the vending machines or in computers of automatic ticket checkers, telephones or various equipment installed in the amusement parks (as recited in appended claims 38 and 39).

As obvious from the foregoing description, the present invention achieves the superior benefit that it can effectively avoid damages which would be caused by

any person stealing or tampering authentication data recorded on recording media.

Examples of Practical Applications:

(Example 1)

Now, the present invention will be described in relation to a case where it is used for mutual authentication between computers on a hierarchical communication network. Fig. 14 is a diagram illustrating a hierarchical network of computers installed within a company. In this example, a host or master computer 41 of the company does not itself contain a unique time generating device; instead, such a unique time generating device is provided in each of the lower-level computers subservient to the master computer 41 (as recited in appended claims 4, 5, 6 and 7). Directly connected to the master computer 41 are the computers 42, 43 and 44 of a sales department, accounting department and administration department. Further, the computers 45, 46, 47 and 48 of individual sales sections are connected to the sales department's computer 42, the computers 49 and 50 of individual accounting sections to the accounting department's computer 43, and the computers 51 and 52 of individual administration sections to the administration department's computer 44. The computers subservient to or under the control of the master computer 41 are interconnected via the network for

intercommunication. Each of the computers other than the master computer 41 is provided with a unique time generating device 42A - 52A. As in the above-described best mode, all of these unique time generating devices 42A to 52A are set to measure unique or different elapsed times at every given time point. Memory 54 of the master computer 41 includes a data memory 55 in which are prestored various data on the unique time generating devices 42A to 52A provided in the individual lower-level computers under the control of the master computer 41. The master computer 41 also includes a CPU 56, a renewal means 57, a collator means 58, a transmitter means 59 and a receiver means 60. The memory 54 of the master computer 41 further includes a register means 61.

Each of the lower-level or subservient computers 42 to 53 includes a CPU 61, a renewal means 62, a transmitter means 63, a receiver means 64, a reading means 65, an authorizing means 66 and a rejecting means 67, as shown in Fig. 16.

For example, when the computer 45 of the first sales section desires to access the computer 50 of the second accounting section to request supply of some accounting-related information, the CPU 61 of the computer 45 creates unique authentication data TKA, peculiar to the computer 45, based on an elapsed time measurement TK indicated by the unique time generating

device 45A and transmits the thus-created unique authentication data to the higher-level sales department's computer 42 via the transmitter means 63 (see Fig. 16). In turn, the sales department's computer 42 forwards the unique authentication data to the receiver means 42 of the master computer 41. Thus, in the master computer 41, the collator means 58 connected to the CPU 56 collates the unique authentication data TKA, received by the master computer 41, with the information on the individual unique time generating devices prestored in the data memory 55, to find which of the subservient computers has created and issued the authentication data TKA. Once the unique authentication data TKA is determined as having been fairly created and issued by any one of the subservient computers as a result of the collation, the master computer 41 registers the authentication data TKA in the register means 61 as part of an up-to-date record or history of unique authentication data issuance by the subservient computer (see Fig. 15). Once the unique authentication data TKA is duly registered in the register means 61, the transmitter means 59 of the master computer 41 transmits information, authorizing the desired access, to the receiver means 64 of the computer 45 of the first sales section by way of the sales department's computer 42.

Thus, in response to the acceptance or authorization of the desired access, the computer 45 of

the first sales section sends, via the transmitter means 63, data to initiate the access to the computer 50 of the second accounting section. At that time, the unique authentication data TKA is sent, as a unique identification of the computer 45, to the receiver means 64 of the computer 50 of the second accounting section along with a request for the accounting-related information.

Then, in the computer 50 of the second accounting section, the reading section 65 reads the unique authentication data TKA from among the received information, and the thus-read authentication data TKA is transmitted from the transmitter means 63, via the accounting department's computer 43, to the receiver means 60 of the master computer 41, where the data TKA is subjected to the collation (see Fig. 16).

In the master computer 41, the collator means 58 collates the received authentication data TKA to determine whether the received data duly matches the data registered in the register means 61. If the authentication data TKA matches the data registered as an up-to-date record or history of issuance of unique authentication data by the subservient computer, the master computer 41 transmits the collated result from its transmitter means 59 to the computer 50 of the second accounting section by way of the accounting department's computer 43.

In this way, the receiver section 64 in the computer 50 of the second accounting section receives the collated unique authentication data TKA. If the collated unique authentication data TKA is judged to be proper data (that has been fairly created and issued by any one of the subservient computers), then the authorizing means 66 in the computer 50 permits further communication with the computer 45 of the first sales section, in response to which the requested accounting-related information is supplied to the computer 45.

If, on the other hand, the collated unique authentication data TKA is judged to be improper data (that has not been fairly created and issued by any one of the subservient computers), then the rejecting means 67 in the computer 50 inhibits further communication with the computer 45 of the first sales section because there is a great likelihood that an unauthorized outsider' computer is pretending to be the computer 45.

With the authentication-data issuing and verifying system in accordance with Example 1 above, each of the computers on the hierarchical network can be authenticated reliably in accordance with data created and issued on the basis of an elapsed time measurement indicated by the unique time generating device provided therein. Thus, it is possible to effectively prevent any third person's computer from unfairly conducting data exchange by pretending to be one of the subservient

computers or intruding into the hierarchical network.

Whereas in Example 1 unique authentication data TKA issued by the computer 45 of the first sales section has been described as being transmitted to the master computer 41 by way of the sales department's computer 42, such data may be transferred directly to the master computer 41. Similarly, data to be collated and resultant collated data may be communicated between the master computer 41 and the computer 50 of the second accounting section directly, rather than by way of the accounting department's computer 43.

Further, when the computer 45 of the first sales section desires further access to the computer 50 of the second accounting section in Example 1, the unique authentication data TKA created and issued earlier may be altered by the renewal section 62 on the basis of an elapsed time measurement indicated by the unique time generating device 45A so that further communication is safely made between the two computers 45 and 50 on the basis of the thus-altered unique authentication data in a similar manner to the above-described best mode. In this case, the renewal means 57 in the master computer 41 may update the unique authentication data registered in the register means 61 (as recited in appended claims 31 and 32). Also, in such a case, the subservient computers may include a memory means (not shown) for storing the unique authentication data (including the

altered unique authentication data) for use in next access. Rather than providing such a memory means in the subservient computers, an alternative arrangement may be made such that the last-issued unique authentication data TKA is read out from register means 61 in the master computer 41 as the computer 45 of the first sales section requests access to the computer 50 of the second accounting section and additional data based on a new elapsed time measurement received from the computer 45 is imparted to the authentication data TKA to thereby create and issue unique authentication data that is updated in both the master and subservient computers.

Moreover, whereas Example 1 has been described as carrying out the further access between the subservient computers on the basis of such updated unique authentication data, unique authentication data may be created and issued, as a so-called one-time password, for each access on the basis of an elapsed time measurement indicated by the unique time generating device provided in the computer requesting the access (as recited in appended claim 9).

Furthermore, in addition to the arrangement of Example 1, the accessed subservient computer may also create and issue unique authentication data via its unique time generating device and transmit the unique authentication data to the accessing computer by way of same procedure as taken for the unique authentication

data of the latter computer, so as to permit mutual authentication between the two computers. Moreover, whereas Example 1 has been described in relation to the case where the computers of the individual sections are the lowest-level computers in the company, still-lower-level computers may be connected to the sections' computers for use at various stations or by individual constituent members belonging to the sections and departments (as recited in appended claim 16).

(Example 2)

Next, the authentication-data issuing and verifying system of the present invention will be described in relation to a case where it is applied to mutual authentication among computers of various banking agencies (as recited in appended claims 10 to 15, 20, 22, 38, 39, etc.) This example assumes that account transfers, settlements of account, etc. between the banking agencies are conducted via the respective computers. Further, in each of the banking agencies, various services to individual customers, such as money changing, loaning, payment into accounts and money withdrawal, are recorded in the computer in association with their account numbers and the like. In Example 2, such various operations between the banking agencies and between the banking agencies and their customers are all executed on the basis of unique authentication data.

Fig. 17 is a diagram illustrating a hierarchical

network of the computers in Example 2, where reference numeral 70 represents a host computer of the central bank (e.g., the Bank of Japan) that functions as a master computer exercising general control of the other computers in the hierarchical network. To the master computer 70 are connected computers of various lower-level or subservient banking agencies, such as host computers 71 of city banks, host computers 72 of local banks, host computers 73 of credit banks and host computers 74 of credit unions —for simplicity, only one host computer is shown and will be described for each of the subservient banking agencies. Further, to the computer of each of the banking agencies are connected host computers of main and local offices and branches, actually performing banking operations, of the associated banking agencies. Furthermore, to the host computer of each of the main and local offices and branches are connected computers of on-line terminals (including cash dispensers). In the computers of the central bank down to the on-line terminals, there are provided unique time generating devices, one for each computer, which count time within different time-measuring periods to indicate different elapsed time measurements at every given time point, as described earlier in relation to the above-described best mode. Data relating to the individual unique time generating devices are stored together in a data memory of the host computer 70 of the central bank

for general management by the host computer 70, similarly to the arrangement of Fig. 15.

Each of the computers on the hierarchical network is arranged to create and issue unique authentication data in a similar manner to the best mode or Example 1, when conducting, via a given terminal computer, a transaction (such as settlement of a draft or check or remittance) with the computer of another banking agency or another office of the same banking agency. For example, when settlement of a check issued by one of the branches of the local bank 72 is requested thereto via the on-line terminal of one of the branches of the city bank 71, a request for access to the branch of the local bank 72 is sequentially made from the on-line terminal, through the city bank's host computer 71, to the central bank's host computer 70. In response to such a request, the central bank's host computer 70 creates and issues authentication data TL1, representative of authorization of the requested access, on the basis of an elapsed time measurement indicated by the unique time generating device provided in that host computer. Then, the local bank's host computer 71 creates and issues authentication data TL2 on the basis of an elapsed time measurement indicated by its unique time generating device and adds the authentication data TL2 to the authentication data TL1 received from the central bank's host computer 70. Thereafter, the branch's computer creates and issues

authentication data TL3 on the basis of an elapsed time measurement indicated by its unique time generating device and adds the authentication data TL3 to the authentication data TL2, and the terminal's computer creates and issues authentication data TL4 on the basis of an elapsed time measurement indicated by its unique time generating device and adds the authentication data TL4 to the authentication data TL3 so as to provide unique authentication data TL1+TL2+TL3+TL4. Thus, the terminal's computer transmits the unique authentication data TL1+TL2+TL3+TL4 to the computer of the local bank's branch as check-settling identification ID along with check settlement information. Prior to the transmission, the issued unique authentication data is sequentially sent to the higher-order computers so that it is registered in register means (not shown) of the branch's and local bank's host computers and ultimately in register means (not shown) of the central bank's host computer 70. The computer of the local bank's branch, having received the check settlement request, reads the unique authentication data TL1+TL2+TL3+TL4 from among the received information and transmits the thus-read data to the higher-order computers so that the data is ultimately collated in the central bank's host computer 70. Specifically, in the central bank's host computer 70, a collator means (not shown) collates the the unique authentication data received from the computer of the

local bank's branch in order to ascertain whether the data matches the authentic data registered in the register means. The collated result is transmitted to the lower-order computers so that it is ultimately received by the branch's computer. If the received data is authentic data, the branch's computer initiates procedures necessary for the check settlement on the basis of permission from the authorizing means; otherwise, it refuses to execute the check settlement procedures.

Details of the individual components in the authentication-data issuing and verifying system are similar to those described earlier in relation to Example 1 and will not be described here to avoid unnecessary duplication.

In the case of a relatively continual transaction, such as an account transfer, remittance or debiting, occurring monthly between the banking agencies (including transactions between the branches and between branches and main office of a same banking agency), unique authentication data used in the last transaction may be updated, as in Example 1, for used in a next transaction. To this end, it is only necessary that authentication data be transmitted from the master computer to the lower-order computers while being imparted unique additional data in each of the lower-order computers so that the lowest-level (terminal)

computer creates and issues updated unique authentication data on the basis of the received authentication data, similarly to the unique authentication data creating procedures of Fig. 17. Registration and verification of such updated unique authentication data are performed in a similar manner to the above-described best mode, Example 1 or modifications (as recited in appended claims 27 to 31) and will not be described here to avoid unnecessary duplication.

Although the updated unique authentication data can be generated by updating the last unique authentication data registered in a renewal means (not shown) of the master computer (host computer 70 of the central bank), a similar renewal means may also be provided in each of the lower-order computers to update the content of the unique authentication data stored in the register means of the lower-order computer (as recited in appended claims 32 and 34). In such a case, the renewal means of each of the lower-order computers may retrieve the updated authentication data registered in the highest-level computer of the central bank to thereby update the last unique authentication data stored in the register means of the lower-order computer (as recited in appended claim 33).

Further, in the example of Fig. 17, each of the banking agencies uses unique authentication data not only in transactions with other banking agencies but also in

direct transactions with their customers. Each of the customers normally holds one or more cards 75 (such as a cash card and credit card) associated with his or her account opened at the banking agency, and it is expected that in the near future the customers will also hold electronic money cards (so-called "electronic money") issued by their banking agencies. Normally, magnetic or IC cards used as such money-equivalent cards are issued via the terminal computers as shown in Fig. 17, at which time unique authentication data is created, for each of the cards, in accordance with elapsed time measurements indicated by the individual unique time generating devices on the basis of original authentication data that is passed from the central bank's computer 70 to the lower-order computers while being imparted additional data in each of the lower-order computers and the thus-created time unique authentication data is recorded onto the card along with other information such as account information (including information on the current balance) and credit information (including information on the maximum limit of loan). Each time the thus-issued card 75 is used in the terminal computer of a selected banking agency to execute any one of various transactions, such as payment into account, money changing, money withdrawal from deposits and savings, deposit of money and inquiry of the current remaining balance, the unique authentication data is collated and

updated in the master computer 70 (or in any of the lower-order computers). Further, for the electronic money cards which are expected to be widely used in the near future, terminal machines (terminal computers) will be installed in shops, department stores, etc. and connected to the network as shown in Fig. 17, and the unique authentication data on the card 75 will be collated and renewed each time it is put to actual use. As a consequence, the money amount in the account corresponding to the card 75 is updated, i.e., increased or decreased, so that various data are created including the up-to-date record of use of the card 75.

With such an arrangement, theft of the recorded data on the card 75 will end in meaningless effort because the recorded data are automatically altered immediately when the card is put to use.

Further, even in a transaction between the central bank and any one of the subservient banking agencies (such as supply of money, particularly that of electronic money, or inquiry or report between the two), reliable authentication is permitted by creating and issuing unique authentication data to carry out necessary procedures on the thus-issued data. Especially, this arrangement allows the central bank's computer to readily know a total money supply (particularly, that of electronic money), so that the monetary policy of the central bank can be properly managed via its host

computer 70. Other arrangements and operation of the example are similar to those of the above-described best mode, example 1 or modifications and will not be described here to avoid unnecessary duplication.

(Example 3)

Fig. 18 is a diagram showing a hierarchical network structure where the authentication-data issuing and verifying system is provided in each of a plurality of computers owned by a railroad company (as recited in appended claims 18, 19, 38, 39, etc.). In the illustrated example, reference numeral 80 represents a host computer of the railroad company, to which are connected subservient computers of individual stations, tourist bureaus and convenience stores --only one station, tourist bureau and convenience store are shown and will be described for simplicity-- that control issuance of railroad tickets. To each of the subservient computers are connected computers contained in or attached to ticket vending machines that issue various tickets with magnetic data recorded thereon, such as ordinary railroad passenger tickets, coupon tickets, commuter passes and platform tickets, as well as prepaid (magnetic) cards for utilizing the railroad facilities. The host computer 80 of the railroad company is also connected with computers of automatic ticket checkers 81 that are placed at the ticket gates of the individual railroad stations to read information recorded on the

prepaid cards and tickets. In this example, a unique time generating device is provided in each of the host computer 80 of the railroad company, computers of the station, tourist bureaus and convenience store and computers of the lowest-level vending machines and ticket checkers 81. Thus, unique authentication data, created and issued by the unique time generating devices on the basis of unique elapsed time measurements in a similar manner to Example 2 above, will be recorded, along with railroad service information indicative of a travel section, type and No. of a reserved seat, term of validity, etc.), onto each of the tickets and prepaid cards sold via the vending machines. To this end, each of the computers of the vending machines and ticket checkers 81 is provided with a reader/writer which reads and write data on the tickets and prepaid cards.

The tickets and prepaid cards issued via the vending machines can be used to pass through the automatic ticket checkers and the prepaid cards can be used to purchase tickets from the vending machines, during which time the unique authentication data recorded on each of these tickets and prepaid cards is read via the reader/writer and then transmitted to the host computer 80 of the railroad company for the subsequent collation. Namely, the host computer 80 collates the received unique authentication data with previously registered data in the register means and then sends the

collated result to the ticket checker 81 or vending machine in which the ticket or prepaid card has been inserted. The ticket checker 81 or vending machine, having received the collated result, permits the use of the ticket or prepaid card if the ticket or prepaid card has been determined as authentic, but otherwise it rejects the use of the ticket or prepaid card. Each of the tickets and prepaid cards thus accepted is subjected to necessary rewriting or updating of the recorded railroad service information and the unique authentication data on the basis of authentication data and the like imparted by the higher-order computers in a similar manner to the above-described best mode and examples. The updated data are sent to the host computer 80 of the railroad company to update the previously registered unique authentication data in the register means thereof. For tickets having a specific term of validity, such as commuter passes and platform tickets, the recorded data may be automatically erased via the register means upon expiration of the term.

Such a system for issuing and authenticating tickets and prepaid cards can of course be applied to other transportation companies than railroad companies, such as airline companies, shipping companies and bus companies. In every such application, it is only necessary that information indicative of the shipping, airline or bus services be recorded on the ticket or

prepaid card along with the unique authentication data. Possible examples of the ticket and prepaid card for use with the present inventive system include cards and tickets for amusement parks, lottery tickets and gift certificates issued by department stores, tickets for various recreational facilities, and tickets for automatic vending machines. In every such case, each amount due is subtracted from the money amount (current balance) recorded on the card or ticket and simultaneously the unique authentication data is updated to thereby prevent unfair or unauthorized use of the card or ticket.

(Example 4)

The identification data issuing and verifying system in accordance with the present invention is also applicable to various other types of transaction card, such as cards issued by credit companies, securities companies, insurance companies, loan companies and trust companies. For example, each card issued by a credit company, as shown in Fig. 19, on the basis of information on the customer's credit standing can be used in every member store of the credit company, and the unique authentication data recorded on the card is of course updated each time the card is used. Further, information on every transaction in the member store is sent, along with the unique authentication data, to a host computer 83 of an associated bank as well as a host

computer 82 of the credit company, so that necessary settlement procedures can be performed between the host computers of the bank and credit company on the basis of the unique authentication data.

(Example 5)

The authentication-data issuing and verifying system in accordance with the present invention is applicable to computers used by an administrative organ (as recited in appended claim 17) as well as companies and other profit-making and non-profit-making organizations as described earlier in relation to Example 1. Namely, in Example 5, a host computer of the administrative organ is set to function as a master computer, and the other computers used at various stations and by constituent members of the organ are made to function as lower-level computers subservient to the master computer. Access between these computers within the administrative organ is carried out on the basis of unique authentication data similarly to the best mode, examples and modifications as described above.

The administrative organ, as shown in Fig. 20, supplies residents with ID cards 85 issued via a card issuing machine 84. At that time, the issuing machine 84 may record unique authentication data created on the basis of respective authentication data transmitted thereto from the host computer 86 and the computer 87 of a main office 86 and added together one after another

(as recited in appended claims 11 and 38). Increased efficiency of the administrative management may be achieved by allowing the residents to get their desired service using the thus-issued ID cards 85 on terminal machines 90 positioned in the main, branch or local office of the administrative organ. In these cases, unfair use of the ID cards by unauthorized persons can be effectively prevented because the unique authentication data recorded on each of the cards is updated immediately every time the card is used on the terminal machine 90.

Whereas the best mode, examples and modifications have been described above mainly in relation to magnetic-type prepaid cards and cash cards, ID cards, etc., the principle of the present invention may also be applied to various other storage media, such as floppy disk and writable CD-ROM. Where the present invention is applied to an IC card, it is possible to incorporate in the IC card a unique time generating device operating on the basis of data received from a higher-level computer, because the IC card can itself contain an electric cell. Further, by attaching the IC card to a handy-type personal computer for connection to communication lines, the computer can work as a lowest-level computer in the hierarchical network structure.

Moreover, whereas the best mode and examples have been described above as communicating the level-specific

authentication data and the ultimate unique authentication data with no particular modification made thereto, it is preferable to encrypt these data via an encoder device. Particularly, it is desirable that these data be appropriately protected from being significantly influenced in a direct manner by a lower-level computer and that the unique time generating devices and their behavior remain invisible.

INDUSTRIAL APPLICABILITY

With the present invention having been described so far, authentication of any one of a plurality of computers interconnected via communication lines or mutual authentication between the computers can be performed with greatly increased accuracy. It is also possible to more accurately authenticate a recording media storing thereon authentication data issued from any of the computers. Further, because the unique authentication data is created and issued or updated or altered every time the recording media having the data stored thereon is put to actual use, the present invention can always grantee a secure transaction even when the unique authentication data is leaked to any third person. Thus, the present invention will find a variety of applications, such as authentication of various money-equivalent transaction instruments such as prepaid cards and cash cards, authentication of tickets,

coupon tickets and electronic money, authentication of personalized ID cards, and computer-based authentication between companies, between banking agencies and between administrative organs.

CLAIMS

1. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, said master computer comprising:

a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

transmitter means for, during communication between said master computer and another of the computers subservient to said master computer, transmitting, from said master computer to the subservient computer, authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device; and

register means for receiving and registering an issuance history of unique authentication data created and issued by said subservient computer imparting

additional data, unique to said subservient computer, to the authentication data transmitted by said master computer.

2. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, said master computer including a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

each of the computers subservient to said master computer comprising:

receiver means for, during communication with said master computer, receiving authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device of said master computer;

issuer means for creating and issuing unique authentication data by imparting additional data, unique

to said subservient computer, to the authentication data received via said receiver means from said master computer; and

transmitter means for transmitting, to said master computer, an issuance history of the unique authentication data created and issued by said issuer means.

3. An authentication-data issuing system as recited in claim 2 wherein said issuer means in each of the subservient computers includes imparting means for imparting the additional data, unique to said subservient computer, to the received authentication data, and said imparting means includes a unique time generating device that includes time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period, and

wherein said unique time generating device in said imparting means indicates elapsed time measurements over the time-measuring period that is different from the time-measuring periods of the unique time generating

devices provided in said master computer and other subservient computers and creates and issues unique authentication data peculiar to said subservient computer.

4. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer comprising:

a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period unique to said computer that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

issuer means for creating and issuing unique authentication data, peculiar to said subservient computer, on the basis of an elapsed time measurement indicated by said unique time generating device; and

transmitter means for transmitting, to said master computer, an issuance history of the unique authentication data created and issued by said issuer

means.

5. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer comprising a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period unique to said computer that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

said master computer, exercising general control of the subservient computers, including register means for receiving and registering an issuance history of data created and issued by each of said subservient computers on the basis of an elapsed time measurement indicated by said unique time generating device of said subservient computer.

6. An authentication-data issuing system as recited in claim 3 or 4 wherein said master computer functions as

an original supplier of unique time to said subservient computers so that said unique time generating devices of said subservient computers are activated to indicate elapsed time measurements within their respective preset time-measuring periods different from each other.

7. An authentication-data issuing system as recited in claim 3 or 4 wherein said master computer functions as an original supplier of unique time to said subservient computers so that said unique time generating devices of said subservient computers are activated to indicate elapsed time measurements within their respective preset time-measuring periods different from each other, and each of the computers that are immediately subservient to said master computer is a second-level computer that functions as a secondary supplier of unique time data to third-level computers subservient to said second-level computer so that the unique time generating devices of said third-level computers are activated to indicate elapsed time measurements within their respective preset time-measuring periods different from each other.

8. An authentication-data issuing system as recited in any one of the preceding claims wherein said master computer includes storage means for storing data on said unique time generating device of each of the subservient computers which include data indicative of the time-

measuring period of said unique time generating device, or

data on attributes of said unique time generating devices of said master computer and each of said subservient computers, or

unique additional data to be imparted, by each of said subservient computers, to the authentication data received from said master computer.

9. An authentication-data issuing system as recited in any one of claims 1 to 7 wherein the unique authentication data created and issued by each of said subservient computers is transmitted to and used by one or more other subservient computers under control of said master computer every time a transaction involving use of the unique authentication data is performed.

10. An authentication-data issuing system as recited in any one of claims 1 to 7 wherein the unique authentication data created and issued by each of said subservient computers includes various information to be transmitted to one or more other subservient computers under control of said master computer, said various information including any of information representative of nature of a transaction, merchandise, settlement of account and credit standing.

11. A recording media having stored thereon unique authentication data created by any one of said subservient computers as recited in any one of claims 1 to 7, said recording media being issued by said subservient computer.

12. A recording media as recited in claim 11 which comprises a floppy disk, IC card, magnetic card or writable CD-ROM.

13. A recording media as recited in claim 11 where the unique authentication data stored thereon includes any of monetary information, information on credit loan, money information indicative of a current balance of deposit or saving in a particular account, and information indicative of permission or refusal of use of an amusement part, game house, recreational facility, a railroad, bus, ship, airplane, telephone, facsimile, automatic vending machine or the like.

14. An authentication-data issuing system as recited in any one of claims 1 to 7 wherein said mater computer is a host computer of a central bank exercising general control of banking operations and said subservient computers are computers of banking agencies such as city, local and credit banks under control of the host computer of the central bank, and wherein a transaction,

such as money supply, settlement, loaning, money changing or payment into account, between any one of the banking agencies and a customer is performed on the basis of unique authentication data created and issued for each transaction.

15. An authentication-data issuing system as recited in any one of claims 1 to 7 wherein said master computer is a host computer of a main office of a banking agency exercising general control of a plurality of branches, local offices and the like of the banking agency and said subservient computers are computers installed in the main office, branches and local offices of the banking agency, and wherein a transaction, such as money supply, settlement, loaning, money changing or payment into account, between any one of the subservient computers and a customer is performed on the basis of unique authentication data created and issued for each transaction.

16. An authentication-data issuing system as recited in any one of claims 1 to 7 wherein said mater computer is a host computer of a main office exercising general control of an organization such as a company or corporation and said subservient computers are computers for use at various stations or by constituent members of the organization, and wherein an operation to be effected

by each of the stations or constituent members is performed on the basis of unique authentication data created and issued by the corresponding subservient computer for each operation.

17. An authentication-data issuing system as recited in any one of claims 1 to 7 wherein said mater computer is a host computer of an administrative organ exercising general control of administrative affairs and said subservient computers are computers for use at various stations or by constituent members of the administrative organ, and wherein an operation to be effected by each of the stations or constituent members is performed on the basis of unique authentication data created and issued by the corresponding subservient computer for each operation.

18. A recording media as recited in claim 11 wherein said mater computer is a host computer of a transportation company exercising general control of operations for issuing various tickets, such as an ordinary passenger ticket, railroad and ship tickets, coupon ticket, commuter pass and airline ticket and said subservient computers are computers contained in vending machines installed in a station, airlines, shipping company, tourist bureau, convenience store and the like, said recording media being employed as the thicket issued

by any one of the vending machines and having stored thereon unique authentication data that is created by said subservient computer of the vending machine every time the ticket is used.

19. A recording media as recited in claim 11 wherein said mater computer is a host computer exercising general control of operations for issuing various prepaid cards for using a railroad, ship, airplane, pachinko game machine, telephone, amusement park and the like and said subservient computers are computers contained in vending machines for issuing the prepaid cards, said recording media being employed as the prepaid card issued by any one of the vending machines and having stored thereon unique authentication data that is created by said subservient computer of the vending machine every time the ticket is used.

20. A recording media as recited in claim 11 wherein said mater computer is a host compute of a central bank exercising general control of operations for issuing electronic money and said subservient computers are computers contained in money issuing machines for issuing electronic money to users, said recording media being employed as the electronic money issued by any one of the money issuing machines and having stored thereon unique authentication data that is created by said

subservient computer of the money issuing machine every time the electronic money is used.

21. A recording media as recited in claim 11 wherein said mater computer is a host compute of an administrative organ exercising general control of public services to be provided to individual residents and said subservient computers are computers contained in card issuing machines for issuing personalized ID cards that are to be used by the individual residents to get the public services, said recording media being employed as the ID card issued by any one of the card issuing machines and having stored thereon unique authentication data that is created by said subservient computer of the vending machine every time the ID card is used.

22. A recording media as recited in claim 11 wherein said mater computer is a host compute exercising general control of operations of a banking agency, credit company, securities company, insurance company, loan company and trust company issuing cards such as a cash card, loan card and credit card and said subservient computers are computers contained in card issuing machines for issuing cards to individual customers, and which is employed as said card issued by any one of the card issuing machines and has stored thereon in magnetic form unique authentication data that is created by said

subservient computer of the money issuing machine every time the card is used.

23. An authentication-data verifying system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer comprising:

reading means for reading unique authentication data issued by any one of the subservient computers on the basis of information received from another of the subservient computers, or reading unique authentication data issued by any one of the subservient computers and recorded on a recording media;

transmitter means for transmitting the unique authentication data read by said reading means to said master computer for subsequent collation thereby; and

receiver means for receiving from said master computer a result of collation between an issuance history of the unique authentication data by each of said subservient computers registered in said master computer and the unique authentication data transmitted by said transmitter means.

24. An authentication-data verifying system including a plurality of computers connected with each other via communication lines with one of said computers set to

function as a master computer, said master computer comprising:

receiver means for receiving unique authentication data transmitted by transmitter means of any one of the computers subservient to said master computer, said unique authentication data being issued by the subservient computer and read by reading means of the subservient computer; and

collator means for collating between the unique authentication data received by said receiver means and an issuance history of the unique authentication data by each of said subservient computers that is registered in said master computer; and

transmitter means for transmitting a result of collation by said collator means to receiver means of the subservient computer.

25. An authentication-data verifying system as recited in claim 23 wherein each of said subservient computers includes rejecting means which when a result of the collation by said collator means of said master computer indicates that the unique authentication data read by said reading means is not present in the issuance history, rejects subsequent access between said subservient computer and another of said subservient computers or rejects use, in said subservient computer, of a recording media having stored thereon the unique

authentication data.

26. An authentication-data verifying system as recited in claim 23 wherein each of said subservient computers includes authorizing means which when a result of the collation by said collator means of said master computer indicates that the unique authentication data read by said reading means is present in the issuance history, authorizes subsequent access between said subservient computer and another of said subservient computers or authorizes use, in said subservient computer, of a recording media having stored thereon the unique authentication data.

27. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data authorized by said authorizing means recited in claim 26 or being connected with a recording media, having stored thereon the unique authentication data whose use is permitted by said authorizing means recited in claim 26,

said master computer comprising a unique time

generating device including time keeping means provided in said master computer for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

each of said subservient computers comprising:

receiver means for, during communication with said master computer, receiving authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device;

issuer means for creating and issuing unique authentication data by imparting additional data, unique to said subservient computer, to the authentication data received via said receiver means; and

transmitter means for transmitting, to said master computer, the unique authentication data created and issued by said issuer means.

28. An authentication-data issuing system as recited in claim 27 wherein said issuer means in each of said subservient computers includes imparting means for imparting, to the received authentication data, the additional data unique to said subservient computer, and

said imparting means includes a unique time generating device that includes time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period, and

wherein said unique time generating device in said imparting means indicates elapsed time measurements over a time-measuring period that is different from time-measuring periods of the unique time generating devices provided in said master computer and other subservient computers and creates and issues unique authentication data peculiar to said subservient computer.

29. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data authorized by said authorizing means recited in claim 26 or being connected

with a recording media, having stored thereon unique authentication data whose use is authorized by said authorizing means recited in claim 26,

each of said subservient computers comprising:

a unique time generating device for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

issuer means for creating and issuing unique-authentication-data updating data, corresponding to the authorized unique authentication data, on the basis of an elapsed time measurement indicated by said unique time generating device; and

transmitter means for transmitting, to said master computer, the unique-authentication-data updating created and issued by said issuer means.

30. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being

accessed by another of the subservient computers on the basis of unique authentication data authorized by said authorizing means recited in claim 26 or being connected with a recording media, having stored thereon unique authentication data whose use is authorized by said authorizing means recited in claim 26,

said master computer comprising:

a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

transmitter means for transmitting to, any one of the subservient computers, authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device; and

renewal means for receiving unique-authentication-data updating data that is created and issued by the subservient computer imparting additional data, unique to the subservient computer, to the authentication data from said transmitter means of said master computer, and altering the unique authentication data on the basis of

the received unique-authentication-data updating data to thereby update an issuance history of the unique authentication data by said subservient computer that is registered in said master computer.

31. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data permitted by said authorizing means recited in claim 26 or being connected with a recording media, having stored thereon the unique authentication data whose use is permitted by said authorizing means recited in claim 26,

said subservient computer including a unique time generating device which includes time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

said master computer including renewal means for

receiving unique-authentication-data updating data that is created and issued by the subservient computer in correspondence with the authorized unique authentication data and altering the unique authentication data on the basis of the received unique-authentication-data updating data to thereby update an issuance history of the unique authentication data by said subservient computer that is registered in said master computer.

32. An authentication-data issuing system as recited in claim 30 or 31 wherein said subservient computer includes renewal means, similar to said renewal means of said master computer, for altering the unique authentication data used for gaining authorization to access to another of the computers or to make use of the recording media, on the basis of the unique-authentication-data updating data.

33. An authentication-data issuing system as recited in claim 32 wherein said renewal means of said subservient computer receives data relating to the issuance history updated by said renewal means of said master computer, in such a way that said subservient computer updates the unique authentication data on the basis of the received data relating to the issuance history.

34. An authentication-data issuing system as recited in claim 32 wherein the unique authentication data updated by said renewal means is stored in memory of the subservient computer, having accessed using last-issued unique authentication data, so that the updated unique authentication data is used for next access to another of the subservient computers.

35. An authentication-data issuing system as recited in claim 32 wherein said renewal means alters last-issued unique authentication data, stored on the recording media used in said subservient computer, on the basis of the created and issued unique-authentication-data updating data.

36. An authentication-data issuing system as recited in any one of claims 14 to 17 wherein the unique authentication data created and issued by said subservient computer contains the unique authentication data updated by said renewal means recited in claim 34.

37. A recording media having stored thereon unique authentication data updated by the unique-authentication-data updating data created and issued in claim 35.

38. An authentication-data issuing system as recited in claim 37 wherein the recording media having stored

thereon updated unique authentication data is the ticket recited in claim 18, prepaid card recited in claim 19, electronic money recited in claim 20, ID card recited in claim 21 or card recited in claim 22, and wherein the subservient computer that stores the updated unique authentication data on said recording media is contained in or attached to an automatic ticket checker or a card reader/writer for a prepaid card, ID card or electronic money.

39. An authentication-data issuing system based on unique time or recording media issued by said authentication-data issuing system as recited in claim 38 wherein the recording media used in said subservient computer is a ticket, electronic money, prepaid card or other card, and wherein information indicative of a current balance calculated by subtracting, from a money amount stored on said recording media, a money amount spent at the time of creation of the updated unique authentication data.

ABSTRACT

In an authentication-data issuing system based on unique time, a master computer (1) creates authentication data on the basis of an elapsed time measurement indicated by an unique time generating device (6) and transmits the created authentication data to a lower-level computer (2A), which further delivers the authenticating data to a still-lower-level computer (3A). The lower-level computer and still-lower-level computer sequentially impart respective unique additional data to the authentication data and then transmits the resultant additional-data-imparted data to a lowest-level vending machine (5). The lowest-level vending machine (5) also imparts its unique additional data to the authentication data, received from the still-lower-level computer, to create unique authentication data and records the thus-created unique authentication data on a prepaid card (20) to be issued thereby. Simultaneously, the ultimately-created unique authentication data is sent from the vending machine, through the still-lower-level computer and lower-level computer, back to the master computer (1) for registration therein. When the thus-issued prepaid card (20) is used on a pachinko machine in a pachinko house under the control of the master computer (1), the pachinko machine reads the unique authentication data recorded on the card, and the thus-read data is collated

with the data registered in the master computer (1) to ascertain the authenticity of the card.

FIG. 1

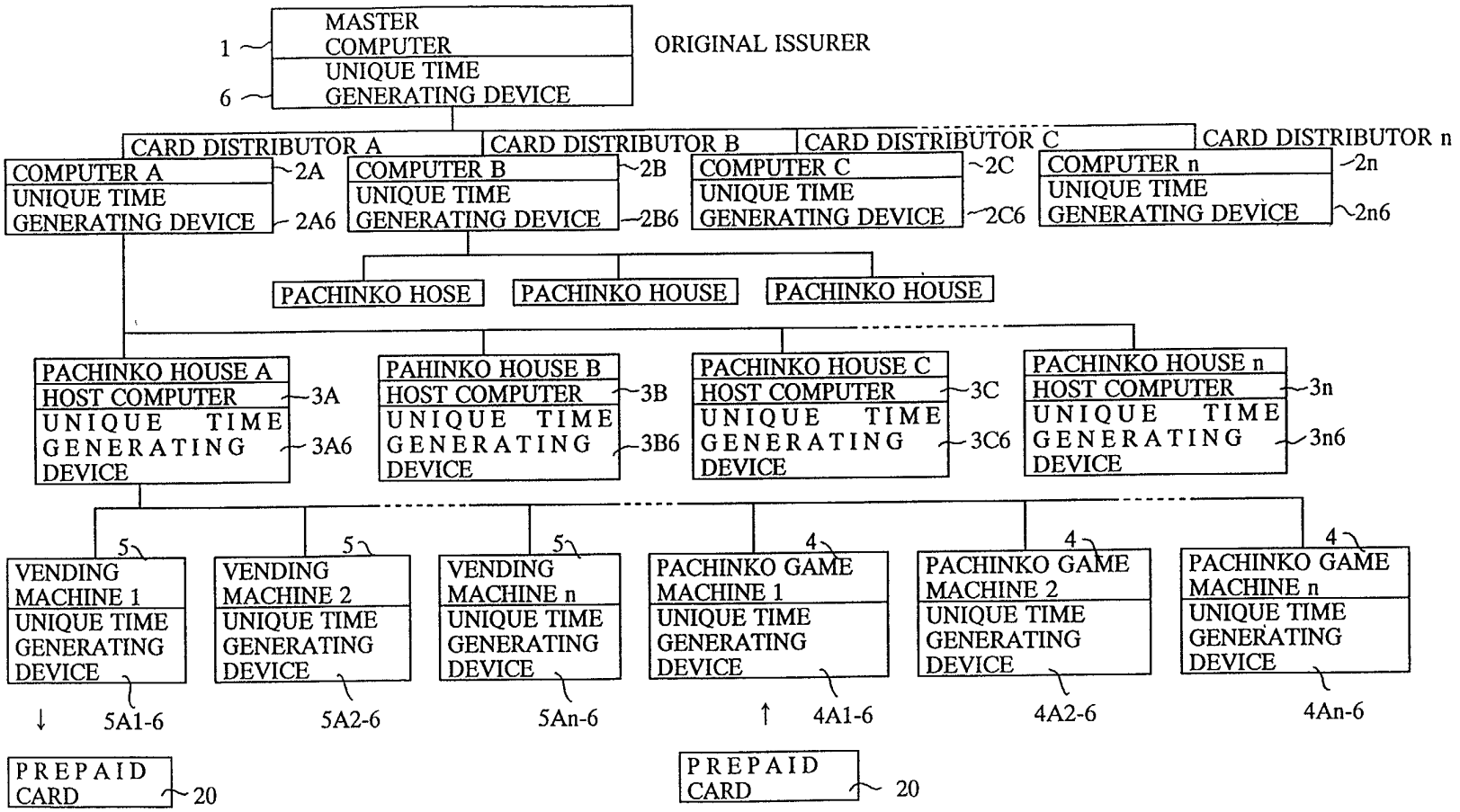

1
MASTER COMPUTER
6
UNIQUE TIME GENERATING DEVICE
ORIGINAL ISSURER
CARD DISTRIBUTOR A
CARD DISTRIBUTOR B
CARD DISTRIBUTOR C
CARD DISTRIBUTOR n
COMPUTER A
UNIQUE TIME GENERATING DEVICE
2A
2A6
COMPUTER B
UNIQUE TIME GENERATING DEVICE
2B
2B6
COMPUTER C
UNIQUE TIME GENERATING DEVICE
2C
2C6
COMPUTER n
UNIQUE TIME GENERATING DEVICE
2n
2n6
PACHINKO HOSE
PACHINKO HOUSE
PACHINKO HOUSE
PACHINKO HOUSE A
HOST COMPUTER
UNIQUE TIME GENERATING DEVICE
3A
3A6
PAHINKO HOUSE B
HOST COMPUTER
UNIQUE TIME GENERATING DEVICE
3B
3B6
PACHINKO HOUSE C
HOST COMPUTER
UNIQUE TIME GENERATING DEVICE
3C
3C6
PACHINKO HOUSE n
HOST COMPUTER
UNIQUE TIME GENERATING DEVICE
3n
3n6
5
VENDING MACHINE 1
UNIQUE TIME GENERATING DEVICE
5A1-6
5
VENDING MACHINE 2
UNIQUE TIME GENERATING DEVICE
5A2-6
5
VENDING MACHINE n
UNIQUE TIME GENERATING DEVICE
5An-6
4
PACHINKO GAME MACHINE 1
UNIQUE TIME GENERATING DEVICE
4A1-6
4
PACHINKO GAME MACHINE 2
UNIQUE TIME GENERATING DEVICE
4A2-6
4
PACHINKO GAME MACHINE n
UNIQUE TIME GENERATING DEVICE
4An-6
PREPAID CARD
20
PREPAID CARD
20

FIG. 2

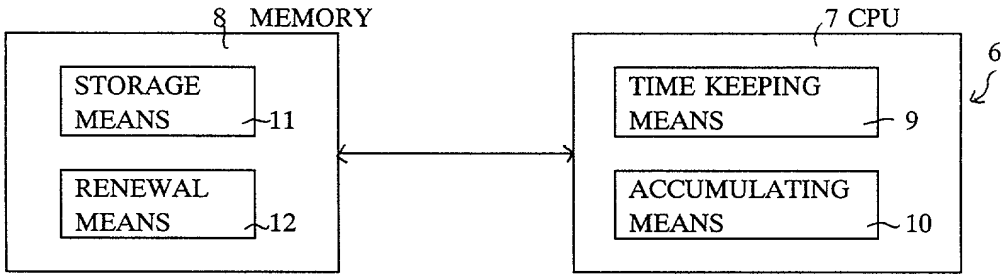


FIG. 3

$$\text{ELAPSED TIME} = \frac{\text{ACCUMULATED TIME } Tn}{\text{TOTAL TIME VALUE } Tt} \Big/ \frac{\text{TOTAL TIME VALUE } Tt}{\text{SUBTRACTED TIME } (Tt - Tn)}$$

ACCUMULATED TIME : (0 → TOTAL TIME VALUE)

SUBTRACTED TIME : (TOTAL TIME VALUE → 0)

FIG. 4

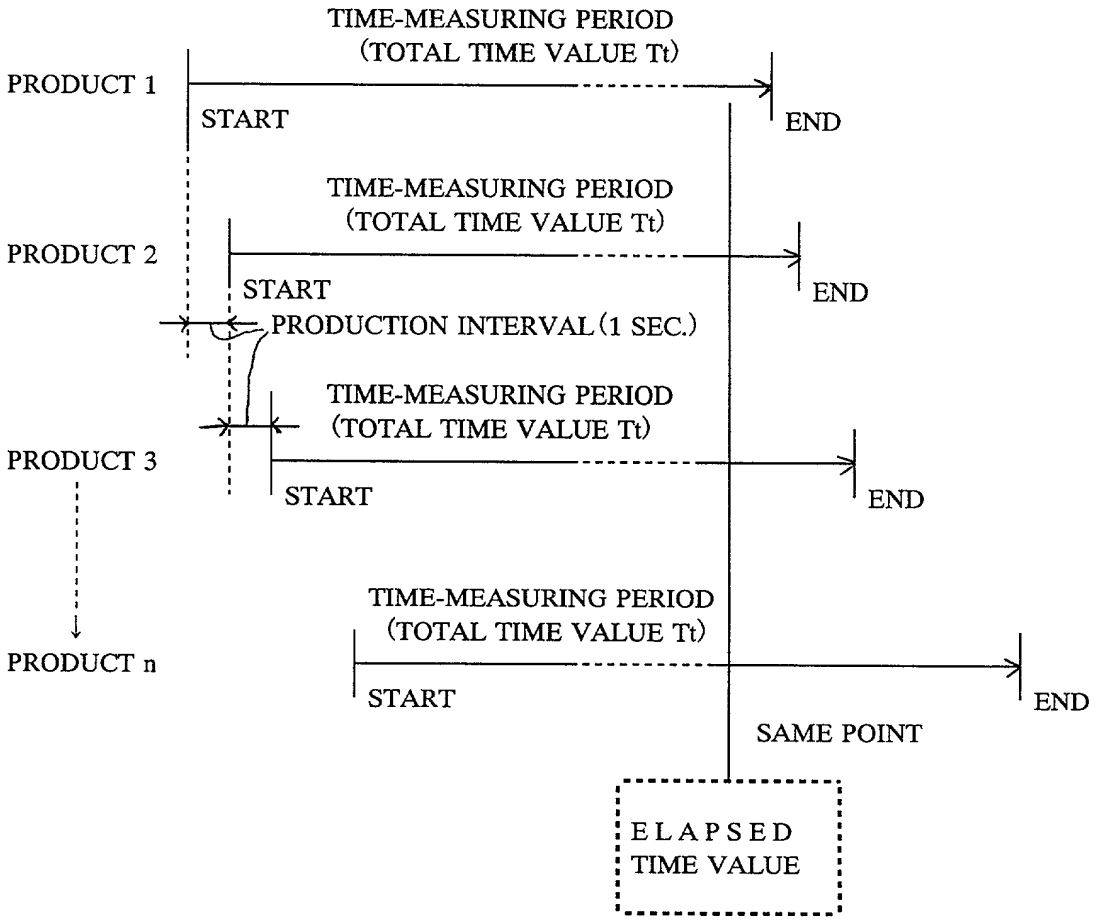

TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt)
PRODUCT 1
START
END
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt)
PRODUCT 2
START
END
PRODUCTION INTERVAL (1 SEC.)
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt)
PRODUCT 3
START
END
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt)
PRODUCT n
START
END
SAME POINT
ELAPSED
TIME VALUE

FIG. 5

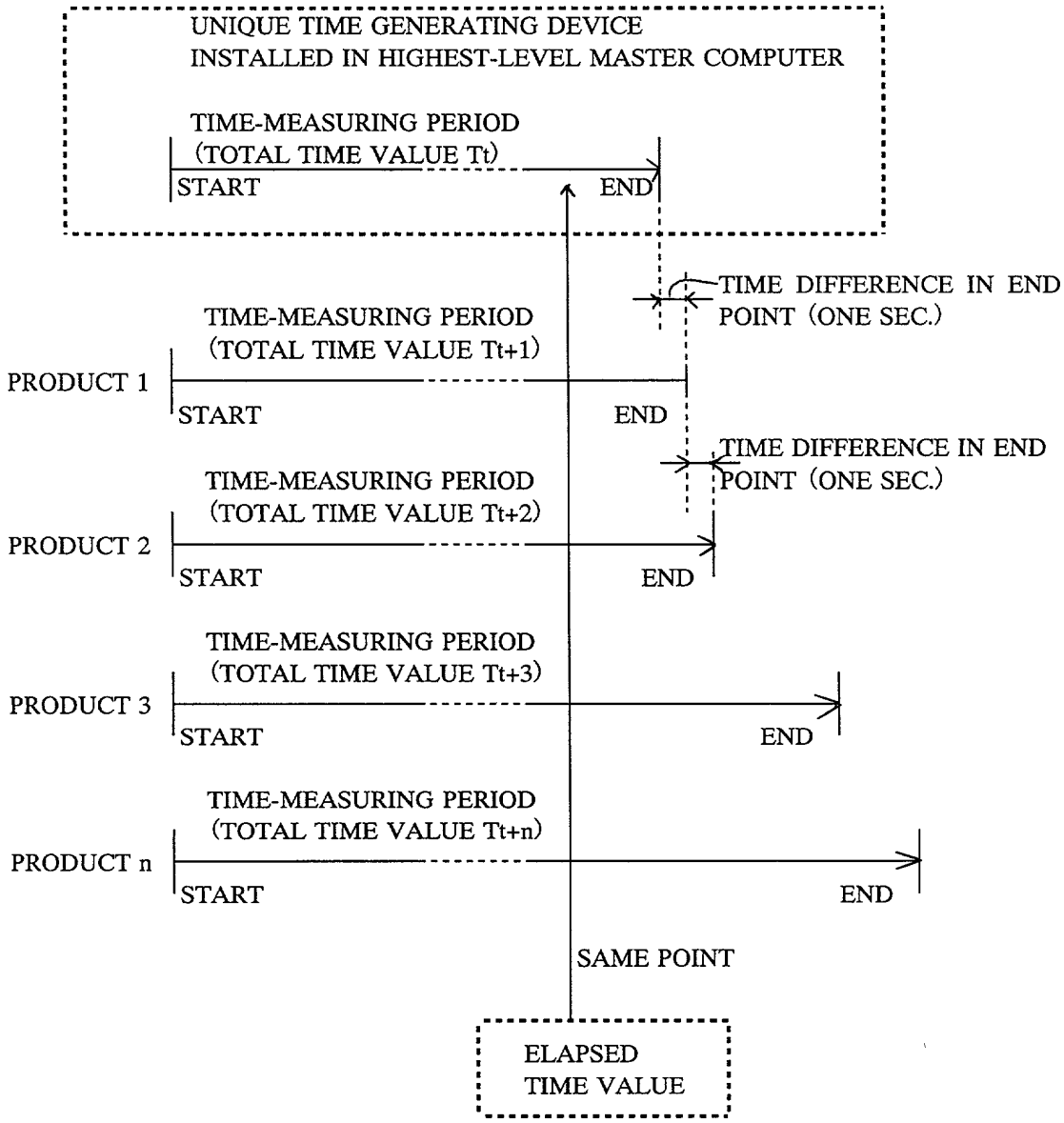

UNIQUE TIME GENERATING DEVICE
INSTALLED IN HIGHEST-LEVEL MASTER COMPUTER
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt)
START
END
TIME DIFFERENCE IN END
POINT (ONE SEC.)
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt+1)
PRODUCT 1
START
END
TIME DIFFERENCE IN END
POINT (ONE SEC.)
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt+2)
PRODUCT 2
START
END
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt+3)
PRODUCT 3
START
END
TIME-MEASURING PERIOD
(TOTAL TIME VALUE Tt+n)
PRODUCT n
START
END
SAME POINT
ELAPSED
TIME VALUE

FIG. 6

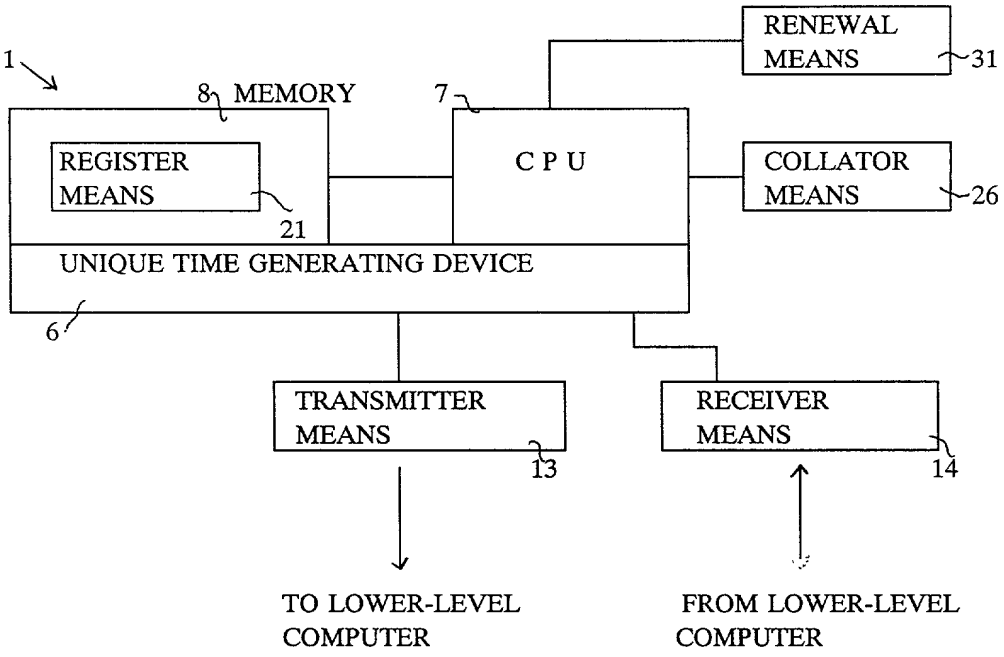

1
8 MEMORY
7
RENEWAL MEANS
31
REGISTER MEANS
21
C P U
COLLATOR MEANS
26
UNIQUE TIME GENERATING DEVICE
6
TRANSMITTER MEANS
13
RECEIVER MEANS
14
TO LOWER-LEVEL COMPUTER
FROM LOWER-LEVEL COMPUTER

FIG. 7

ELAPSED TIME MEASURED BY UNIQUE TIME GENERATING DEVICE 6				AUTHENTICATION DATA
ELAPSED TIME X1	→	ISSUANCE-AUTHORIZING ID FOR 5,000 1,000-YEN CARDS	→	AUTHENTICATION DATA X1a
ELAPSED TIME X2	→	ISSUANCE-AUTHORIZING ID FOR 300 5,000-YEN CARDS	→	AUTHENTICATION DATA X2a
ELAPSED TIME X3	→	ISSUANCE-AUTHORIZING ID FOR 100 10,000-YEN CARDS	→	AUTHENTICATION DATA X3a

FIG. 8

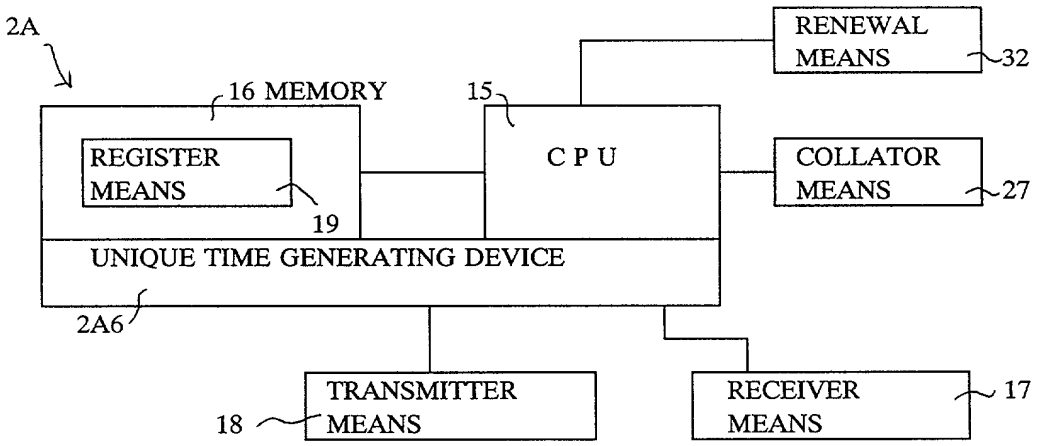


FIG. 9

ISSUANCE OF IDENTIFICATION DATA TO PACHINKO HOUSE A

AUTHORIZED ISSUANCE	AUTHENTICATION DATA ISSUED FROM MASTER COMPUTER	ADDITIONAL AUTHENTICATION DATA BASED ON ELAPSED TIME MEASUREMENT BY COMPUTER 2A	AUTHENTICATION DATA TO BE ISSUED
1,000 × 1,000-YEN PREPAID CARD	X1a	A1 ⋮ A1000	X1a+A1 X1a+A2 X1a+A3 ⋮ X1a+A1000
100 × 5,000-YEN PREPAID CARD	X2a	B1 ⋮ B100	X2a+B1 X2a+B2 X2a+B3 ⋮ X1a+B100
20 × 10,000-YEN PREPAID CARD	X3a	C1 ⋮ C20	X3a+C1 X3a+C2 X3a+C3 ⋮ X3a+C20

FIG. 10

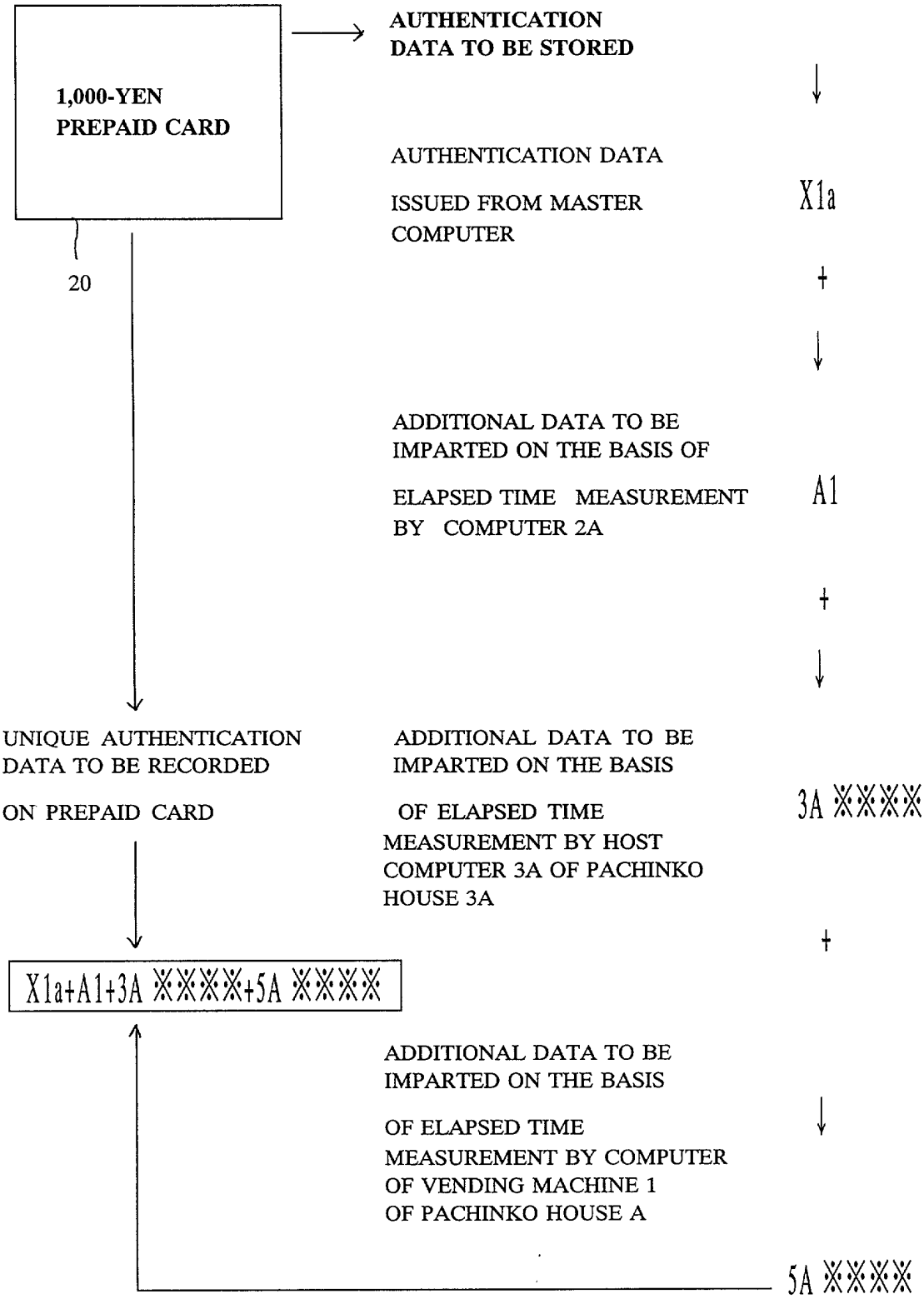

1,000-YEN
PREPAID CARD
20
AUTHENTICATION
DATA TO BE STORED
AUTHENTICATION DATA
ISSUED FROM MASTER
COMPUTER
X1a
+
ADDITIONAL DATA TO BE
IMPARTED ON THE BASIS OF
ELAPSED TIME MEASUREMENT
BY COMPUTER 2A
A1
+
UNIQUE AUTHENTICATION
DATA TO BE RECORDED
ON PREPAID CARD
ADDITIONAL DATA TO BE
IMPARTED ON THE BASIS
OF ELAPSED TIME
MEASUREMENT BY HOST
COMPUTER 3A OF PACHINKO
HOUSE 3A
3A ※※※※
+
X1a+A1+3A ※※※※+5A ※※※※
ADDITIONAL DATA TO BE
IMPARTED ON THE BASIS
OF ELAPSED TIME
MEASUREMENT BY COMPUTER
OF VENDING MACHINE 1
OF PACHINKO HOUSE A
5A ※※※※

FIG. 11

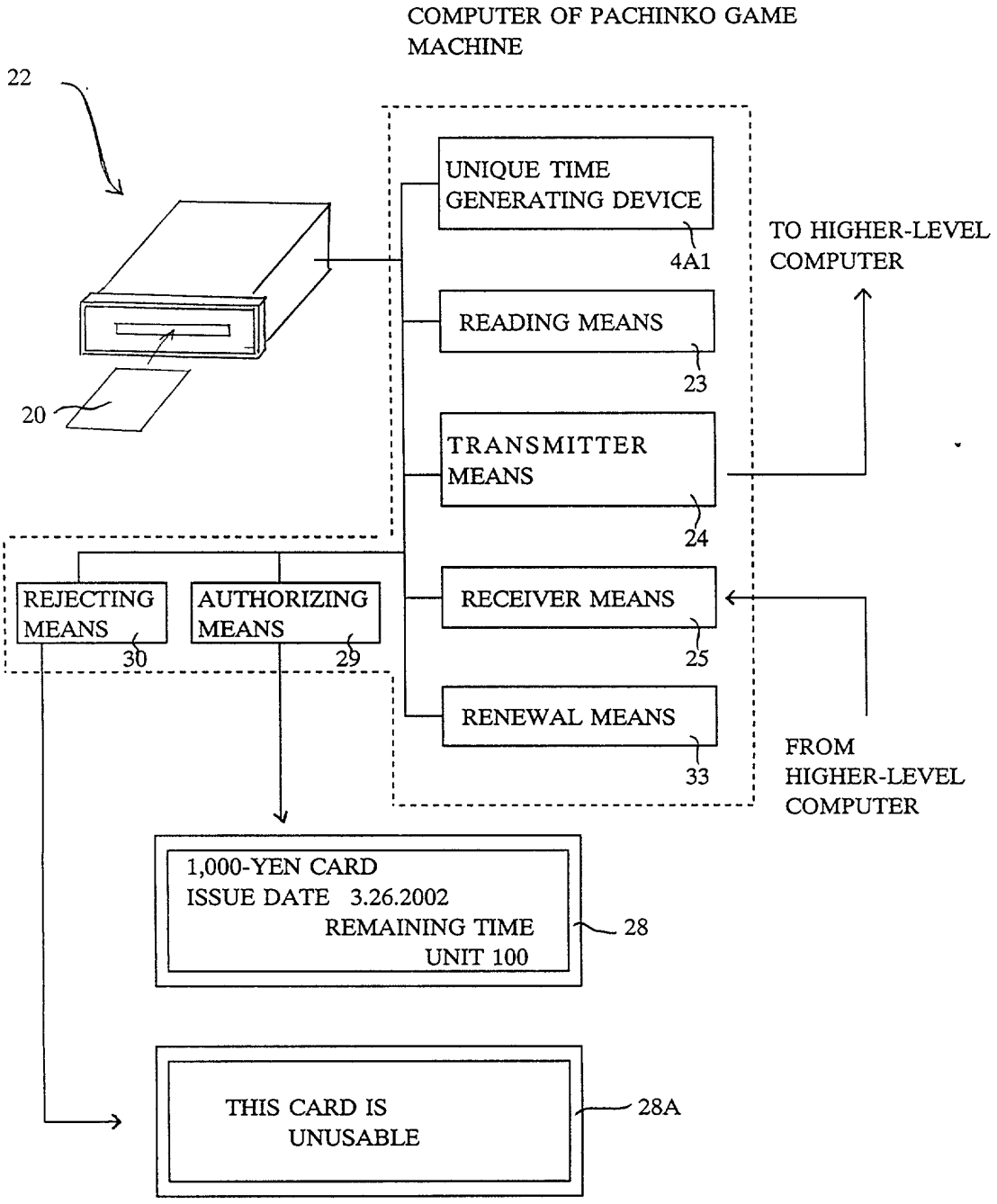

COMPUTER OF PACHINKO GAME MACHINE
22
20
UNIQUE TIME GENERATING DEVICE
4A1
READING MEANS
23
TRANSMITTER MEANS
24
RECEIVER MEANS
25
RENEWAL MEANS
33
TO HIGHER-LEVEL COMPUTER
FROM HIGHER-LEVEL COMPUTER
REJECTING MEANS
30
AUTHORIZING MEANS
29
1,000-YEN CARD
ISSUE DATE 3.26.2002
REMAINING TIME
UNIT 100
28
THIS CARD IS UNUSABLE
28A

FIG. 12

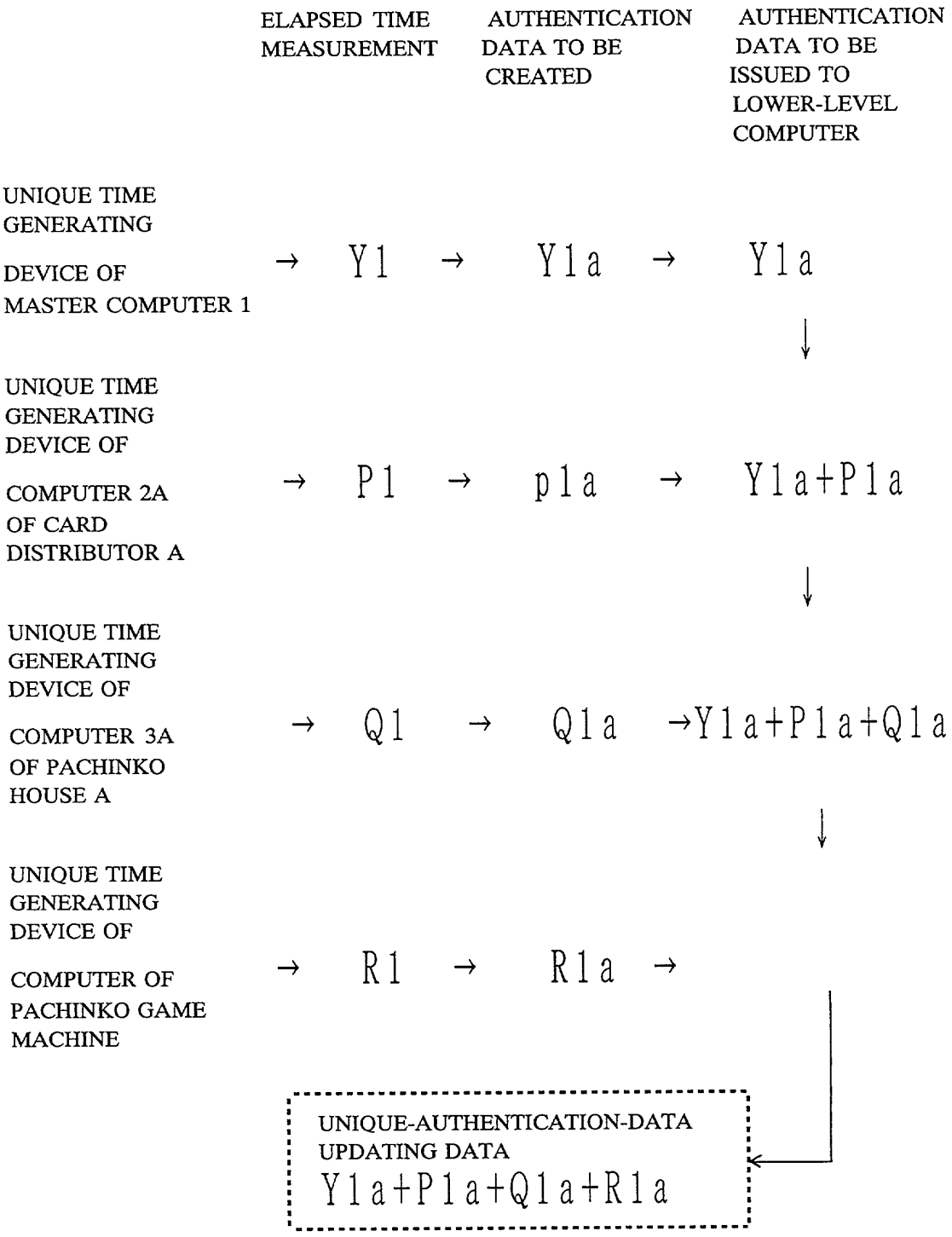

ELAPSED TIME MEASUREMENT
AUTHENTICATION DATA TO BE CREATED
AUTHENTICATION DATA TO BE ISSUED TO LOWER-LEVEL COMPUTER
UNIQUE TIME GENERATING DEVICE OF MASTER COMPUTER 1
→ Y1 → Y1a → Y1a
UNIQUE TIME GENERATING DEVICE OF COMPUTER 2A OF CARD DISTRIBUTOR A
→ P1 → p1a → Y1a+P1a
UNIQUE TIME GENERATING DEVICE OF COMPUTER 3A OF PACHINKO HOUSE A
→ Q1 → Q1a →Y1a+P1a+Q1a
UNIQUE TIME GENERATING DEVICE OF COMPUTER OF PACHINKO GAME MACHINE
→ R1 → R1a →
UNIQUE-AUTHENTICATION-DATA UPDATING DATA
Y1a+P1a+Q1a+R1a

FIG. 13

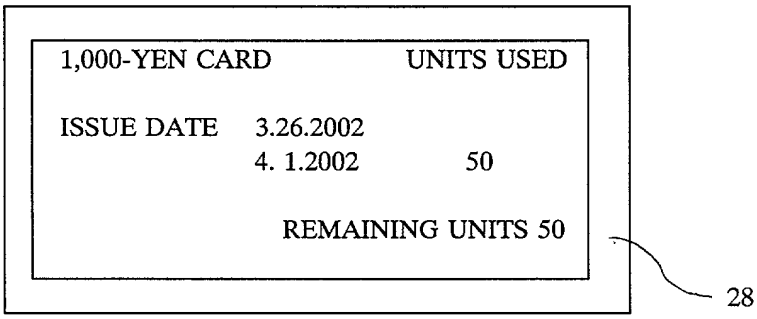

1,000-YEN CARD
UNITS USED
ISSUE DATE
3.26.2002
4. 1.2002
50
REMAINING UNITS 50
28

FIG. 14

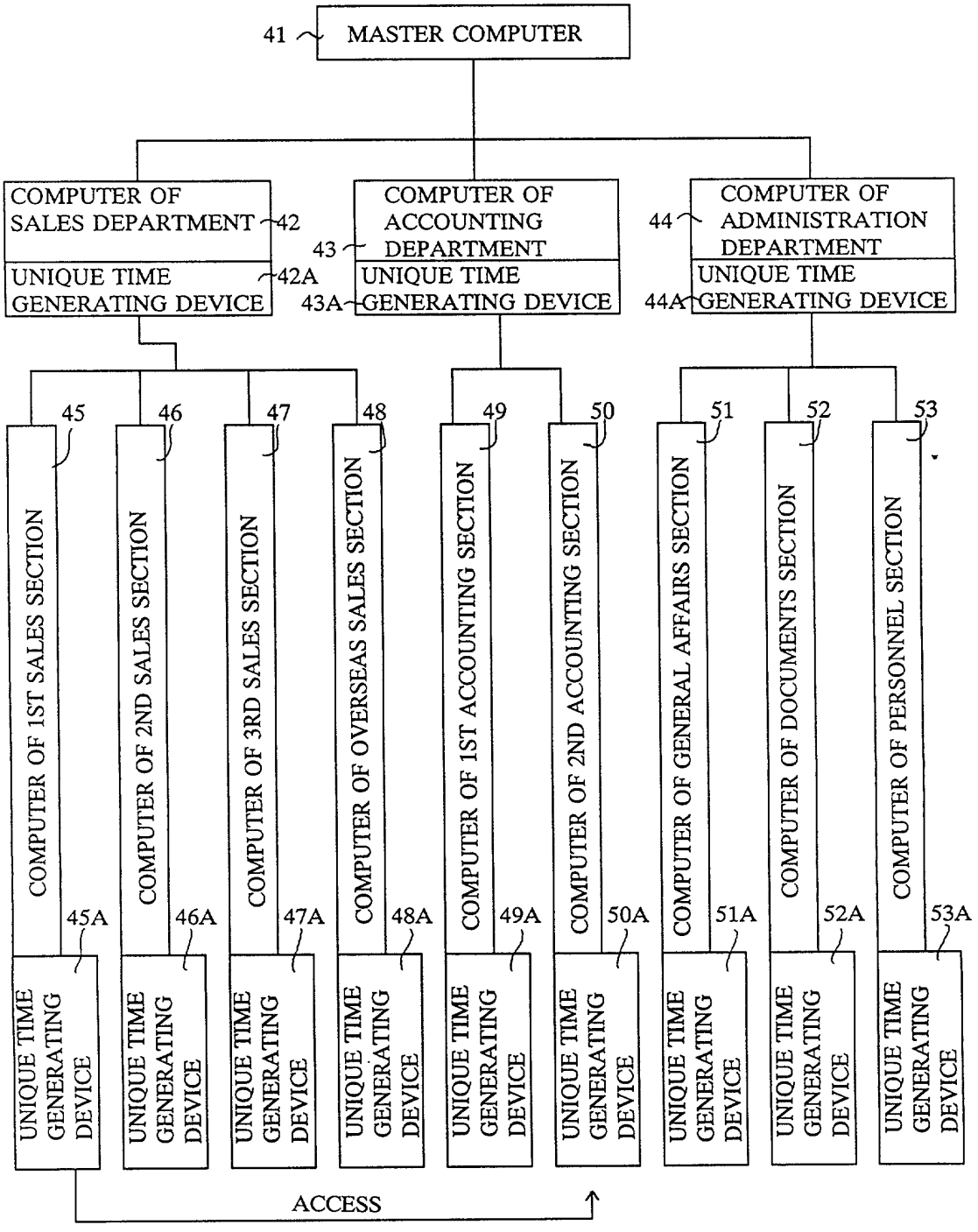

41
MASTER COMPUTER
COMPUTER OF SALES DEPARTMENT
42
UNIQUE TIME GENERATING DEVICE
42A
43
COMPUTER OF ACCOUNTING DEPARTMENT
UNIQUE TIME GENERATING DEVICE
43A
44
COMPUTER OF ADMINISTRATION DEPARTMENT
UNIQUE TIME GENERATING DEVICE
44A
45
COMPUTER OF 1ST SALES SECTION
45A
46
COMPUTER OF 2ND SALES SECTION
46A
47
COMPUTER OF 3RD SALES SECTION
47A
48
COMPUTER OF OVERSEAS SALES SECTION
48A
49
COMPUTER OF 1ST ACCOUNTING SECTION
49A
50
COMPUTER OF 2ND ACCOUNTING SECTION
50A
51
COMPUTER OF GENERAL AFFAIRS SECTION
51A
52
COMPUTER OF DOCUMENTS SECTION
52A
53
COMPUTER OF PERSONNEL SECTION
53A
UNIQUE TIME GENERATING DEVICE
ACCESS

FIG. 15

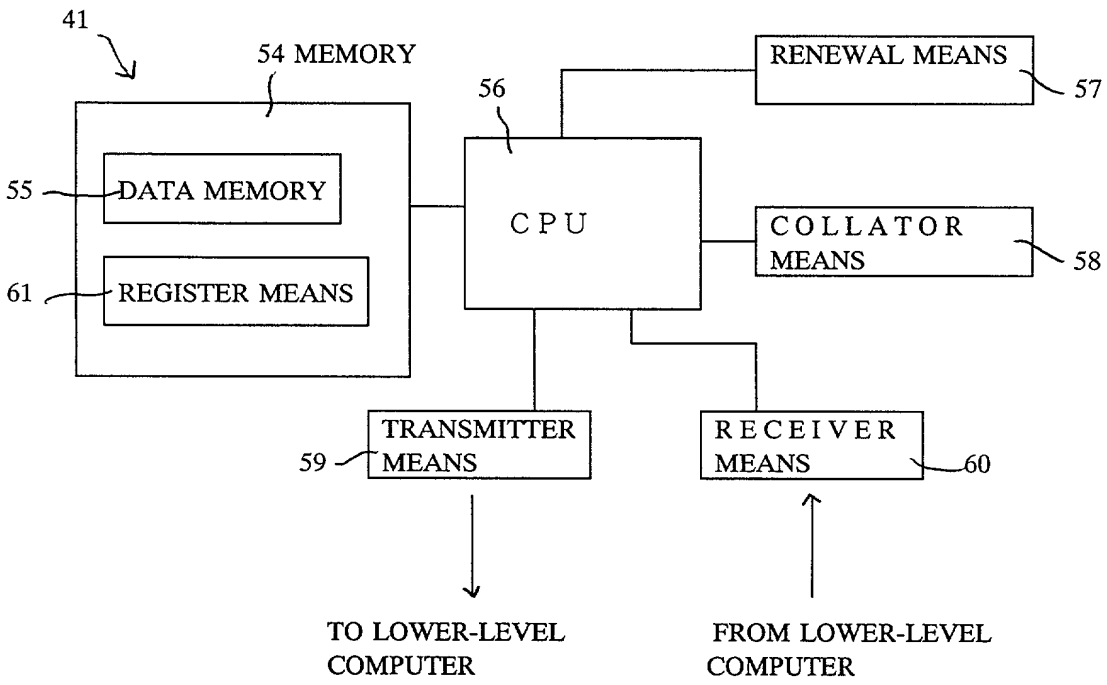

41
54 MEMORY
55
DATA MEMORY
61
REGISTER MEANS
56
CPU
RENEWAL MEANS
57
COLLATOR MEANS
58
59
TRANSMITTER MEANS
RECEIVER MEANS
60
TO LOWER-LEVEL COMPUTER
FROM LOWER-LEVEL COMPUTER

FIG. 16

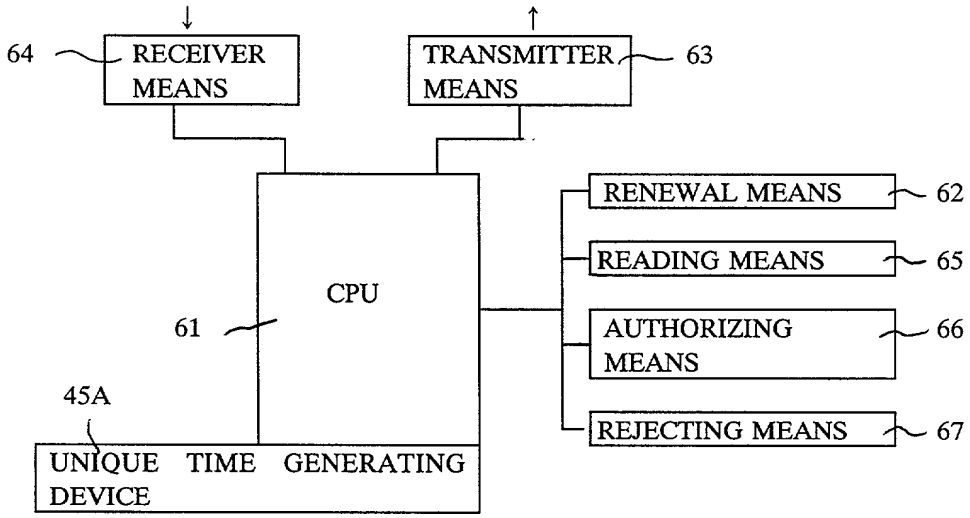

64
RECEIVER MEANS
TRANSMITTER MEANS
63
CPU
61
RENEWAL MEANS
62
READING MEANS
65
AUTHORIZING MEANS
66
REJECTING MEANS
67
45A
UNIQUE TIME GENERATING DEVICE

FIG. 17

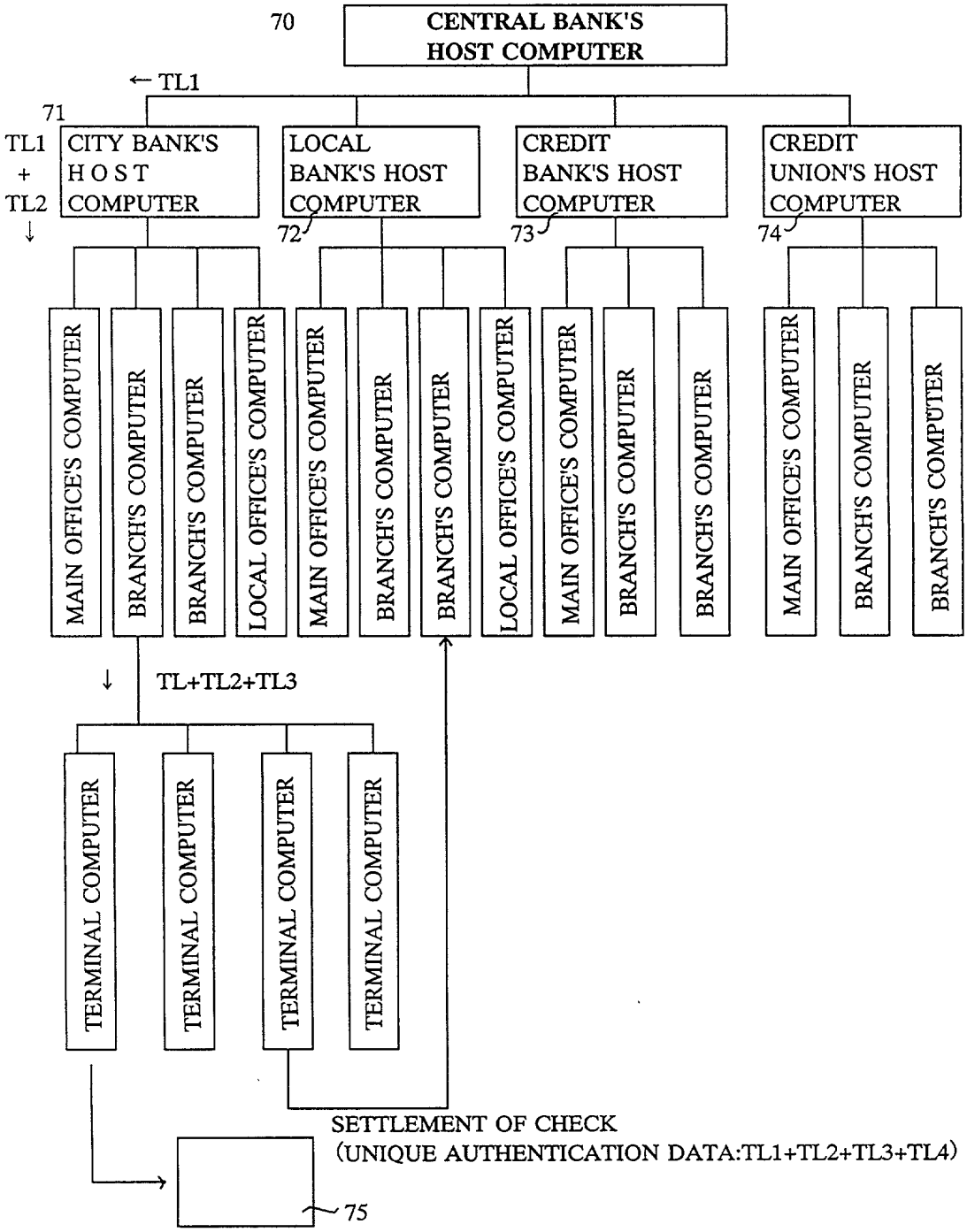

70
CENTRAL BANK'S HOST COMPUTER
← TL1
71
TL1 + TL2 ↓
CITY BANK'S HOST COMPUTER
LOCAL BANK'S HOST COMPUTER
CREDIT BANK'S HOST COMPUTER
CREDIT UNION'S HOST COMPUTER
72
73
74
MAIN OFFICE'S COMPUTER
BRANCH'S COMPUTER
BRANCH'S COMPUTER
LOCAL OFFICE'S COMPUTER
MAIN OFFICE'S COMPUTER
BRANCH'S COMPUTER
BRANCH'S COMPUTER
LOCAL OFFICE'S COMPUTER
MAIN OFFICE'S COMPUTER
BRANCH'S COMPUTER
BRANCH'S COMPUTER
MAIN OFFICE'S COMPUTER
BRANCH'S COMPUTER
BRANCH'S COMPUTER
↓ TL+TL2+TL3
TERMINAL COMPUTER
TERMINAL COMPUTER
TERMINAL COMPUTER
TERMINAL COMPUTER
SETTLEMENT OF CHECK
(UNIQUE AUTHENTICATION DATA:TL1+TL2+TL3+TL4)
75

FIG. 18

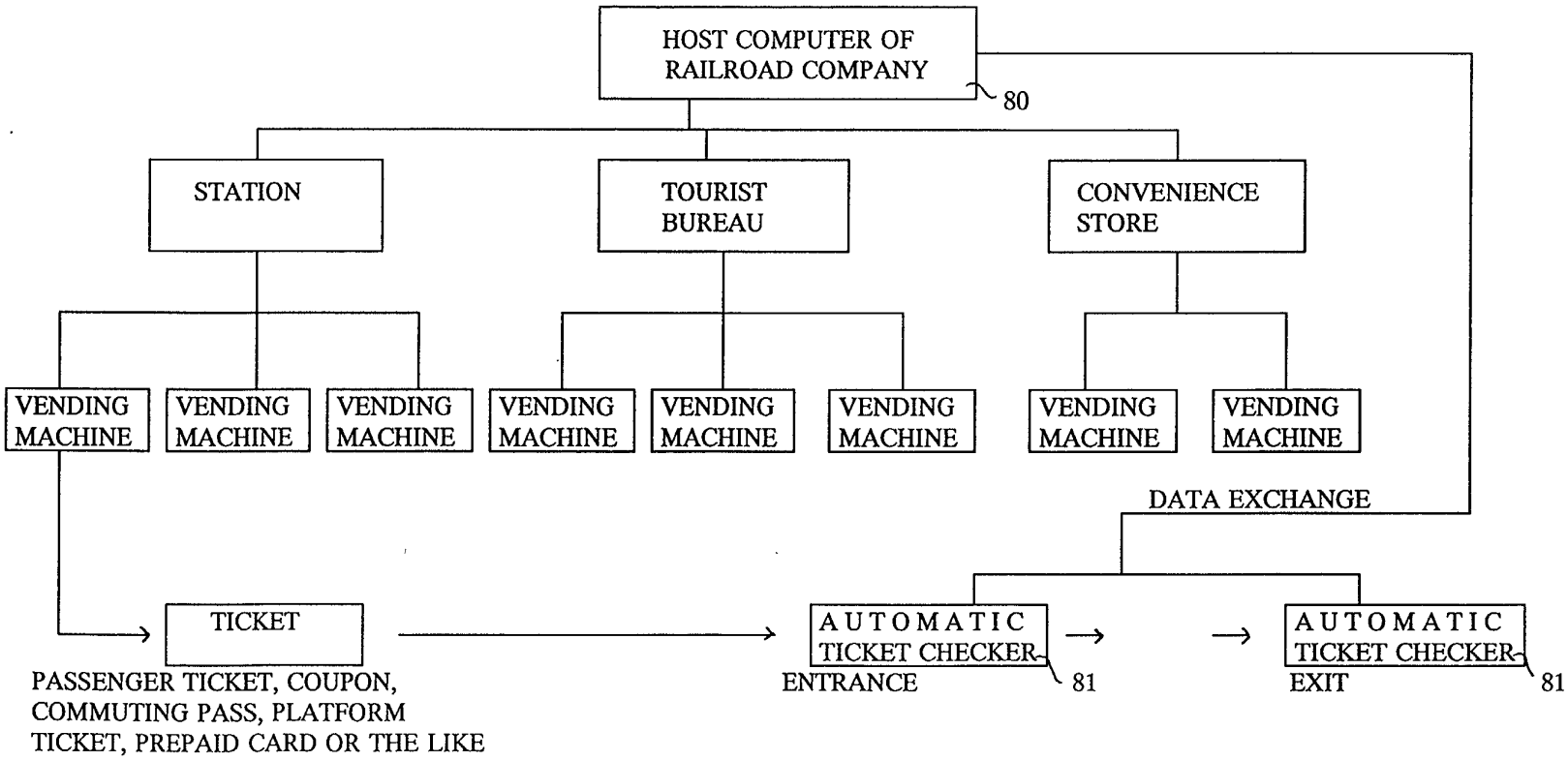

HOST COMPUTER OF RAILROAD COMPANY
80
STATION
TOURIST BUREAU
CONVENIENCE STORE
VENDING MACHINE
VENDING MACHINE
VENDING MACHINE
VENDING MACHINE
VENDING MACHINE
VENDING MACHINE
VENDING MACHINE
VENDING MACHINE
DATA EXCHANGE
TICKET
PASSENGER TICKET, COUPON, COMMUTING PASS, PLATFORM TICKET, PREPAID CARD OR THE LIKE
AUTOMATIC TICKET CHECKER
ENTRANCE
81
AUTOMATIC TICKET CHECKER
EXIT
81

FIG. 19

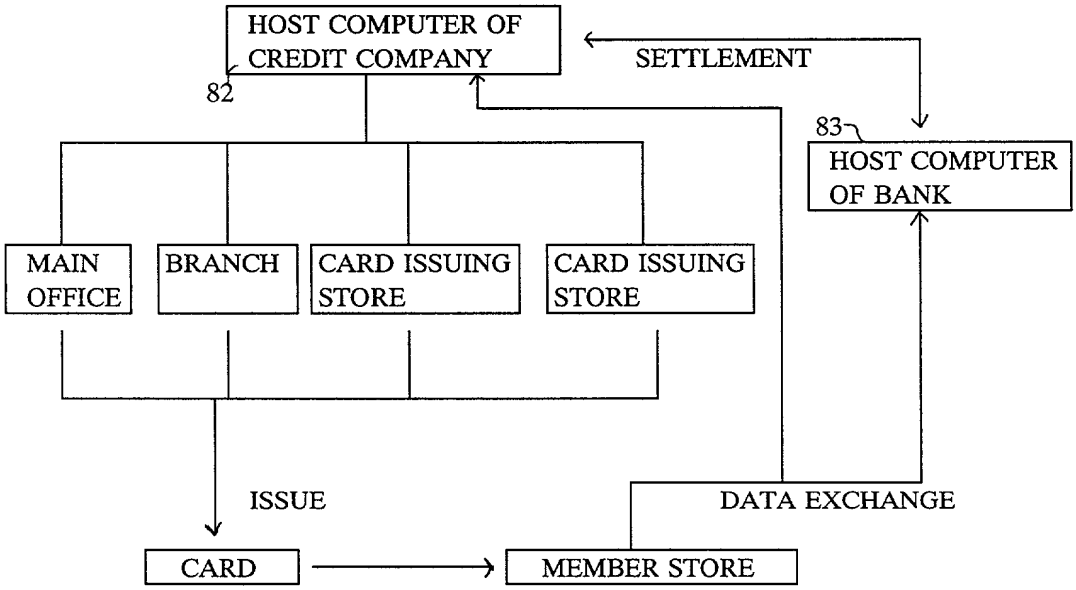
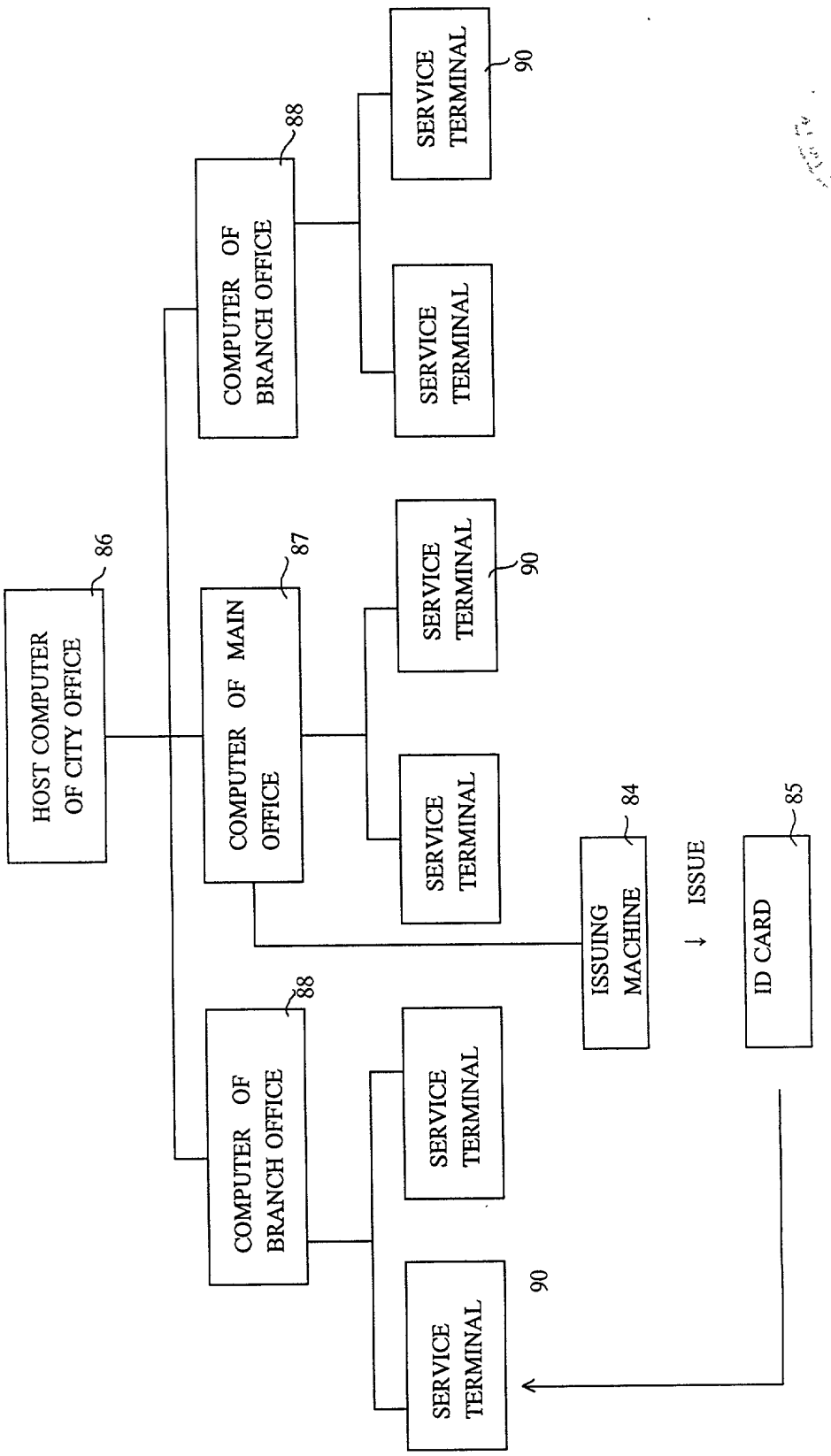

HOST COMPUTER OF CREDIT COMPANY
82
SETTLEMENT
83
HOST COMPUTER OF BANK
MAIN OFFICE
BRANCH
CARD ISSUING STORE
CARD ISSUING STORE
ISSUE
DATA EXCHANGE
CARD
MEMBER STORE

FIG. 20


HOST COMPUTER OF CITY OFFICE
86
COMPUTER OF MAIN OFFICE
87
COMPUTER OF BRANCH OFFICE
88
COMPUTER OF BRANCH OFFICE
88
SERVICE TERMINAL
90
SERVICE TERMINAL
90
SERVICE TERMINAL
90
SERVICE TERMINAL
90
SERVICE TERMINAL
90
ISSUING MACHINE
84
ISSUE
ID CARD
85

Docket No. 051508/0103

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

UNIQUE TIME GENERATING DEVICE AND AUTHENTICATING DEVICE USING THE SAME

the specification of which is attached hereto unless the following box is checked:

☒ was filed on ***March 24, 1997*** as United States Application Number or PCT International Application Number ***PCT/JP97/00972*** and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

NUMBER	COUNTRY	DAY/MONTH/YEAR FILED	PRIORITY CLAIMED

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

APPLICATION NO.	FILING DATE

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS: PATENTED, PENDING, ABANDONED

I hereby appoint as my attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Stephen A. Bent, Reg. No. 29,768; David A. Blumenthal, Reg. No. 26,257; William T. Ellis, Reg. No. 26,874; John J. Feldhaus, Reg. No. 28,822; Patricia D. Granados, Reg. No. ~~33,683~~; John P. Isacson, Reg. No. ~~33,715~~; Donald D. Jeffery, Reg. No. 19,980; Eugene M. Lee, Reg. No. 32,039; Richard Linn, Reg. No. 25,144; Peter G. Mack, Reg. No. 26,001; Brian J. McNamara, Reg. No. 32,789; Sybil Meloy, Reg. No. 22,749; George E. Quillin, Reg. No. 32,792; Colin G. Sandercock, Reg. No. 31,298; Bernhard D. Saxe, Reg. No. 28,665; Charles F. Schill, Reg. No. 27,590; Richard L. Schwaab, Reg. No. 25,479; Arthur Schwartz, Reg. No. 22,115; Harold C. Wegner, Reg. No. 25,258.

19

Address all correspondence to FOLEY & LARDNER, 3000 K Street, N.W., Suite 500, Washington, DC 20007-5109. Address telephone communications to *Arthur Schwartz* at (202) 672-5300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First or Sole Inventor	Signature of First or Sole Inventor	Date
Akira SUGIYAMA	A. Sugiyama	December 9, 1998
Residence Address *Kanagawa, Japan* JPX	Country of Citizenship *Japan*	
Post Office Address *Fujinokidaidanchi 27-102 1, sugesengoku 3-chome Tama-Ku, Kanagawa, 214 JAPAN*		